UNIVERSITY OF OULU

DEGREE PROGRAMME IN WIRELESS COMMUNICATIONS ENGINEERING

MASTER'S THESIS

PERFORMANCE MEASUREMENTS OF BLUETOOTH 5 TECHNIQUE UNDER INTERFERENCE

Author	Dinesh Acharya
Supervisor	Dr. Heikki Karvonen
Second Examiner	Prof. Jari Iinatti

November, 2019

Acharya D. (2019) Performance measurements of Bluetooth 5 technique under interference. University of Oulu, Degree Programme in Wireless Communications Engineering. Master's Thesis, 59 p.

ABSTRACT

This thesis focuses on experimental performance of the Bluetooth 5 technology and compares results with the previous version. Bluetooth technology, institute of electrical and electronics engineers (IEEE) Std. 802.15.4, and other techniques share the same unlicensed 2.4 GHz industrial, scientific, and medical (ISM) spectrum. Various technologies are operating in the same frequency band, and if the channel utilized by these technologies overlap, end in Cross-technology interference (CTI).

Measurements have been performed in indoor scenario and ZigBee nodes were used as an interference. Performance output of the Bluetooth 5 is compared to a previous release Bluetooth low energy (BLE) 4 which is currently one of the popular technologies in commercial wireless devices and expected to be even more widespread in the future. This new Bluetooth technology has featured increased data rate, low power consumption, longer range, higher broadcasting capacity, and improved coexistence with other wireless technologies operating in the same frequency band. The main goal of this work was to evaluate the experimental communication range and throughput of the BLE 5 coded version under interference. Nordic Semiconductor nRF52840 chipset has been used for measurement and result shows the practical communication range and throughput of BLE 5 coded version under interference. In this work, with coding, one-third BLE link gain was achieved when considering packet error rate (PER) less than 10%. In addition, ZigBee interference was found to be harmful for the Bluetooth communication when operating in the same frequency band.

Key words: IEEE, CTI, BLE, Coded, Coexistence, nRF52840, PER, ZigBee.

TABLE OF CONTENTS

FOREWORD

This thesis project has been carried out as a partial fulfilment for the completion of degree towards the master's degree Programme in Wireless Communications Engineering, at Centre for Wireless Communications, University of Oulu, Finland.

I would like to thank my advisor, Dr. Heikki Karvonen for his guidance, support, comments, and reviews during the thesis project. I would like to pay my gratitude to Prof. Jari Iinatti for his reviews and suggestions. A special thanks to Dr. Konstantin Mikhaylov for the technical support. My gratitude towards Moklesur Rahman, who stayed with me during the measurement time and help in physical movement of measurement devices.

I would like to dedicate this thesis to my parents and sisters for their unconditional love, encouragement, and support.

Dinesh Acharya
November 2019, Oulu, Finland

LIST OF ABBREVIATIONS AND SYMBOLS

AFH	adaptive frequency hopping
AWGN	additive white Gaussian noise
ANT	adaptive network technology
API	application programming interface
ATT	attribute protocol
BR	basic rate
BIs	beacons intervals
BPSK	binary phase shift keying
BER	bit error rate
BLE	Bluetooth low energy
BAN	body area network
CSMA/CA	carrier sense multiple access/ collision avoidance
CDMA	code division multiple access
WCDMA	wideband CDMA
COM	communication
COMP	comparator
CCK	complementary code keying
CE	connection event
CIs	connection intervals
CTI	cross-technology interference
DK	development kit
DPSK	differential phase shift keying
DQPSK	differential quadrature phase shift keying
DSSS	direct sequence spread spectrum
EDR	enhanced data rate
eSCO	extended synchronous oriented
FDMA	frequency division multiple access
FH	frequency hopping
FHSS	frequency hopping spread spectrum
FM	frequency modulation
GFSK	Gaussian frequency shift keying
GPIOs	general purpose input/ output
GAP	generic access profile
GATT	generic attribute profile
GPS	global positioning system
HS	high speed
HCI	host controller interface
HID	human interface device
ID	identification
ISM	industrial, scientific, and medical
IEEE	institute of electrical and electronics engineer

IoT	internet of things
LSB	least significant byte
LEDs	light emitting diodes
LOS	line of sight
LL	link layer
L2CAP	logical link control and adaptation layer protocol
LDO	low-dropout regulator
LE	low energy
MSD	mass storage device
MAC	media access control
MCU	micro controller unit
MWS	mobile wireless standard
MSB	most significant byte
NFC	near field communication
NLOS	non-line of sight
O-QPSK	offset-quadrature phase shift keying
OFDM	orthogonal frequency division multiplexing
PDU	packet data unit
PEP	packet error probability
PER	packet error rate
PAN	personal area network
PSK	phase shift keying
PHY	physical layer
PCB	printed circuit board
QoS	quality-of-service
RF	radio frequency
RFID	radio frequency identification
RAM	random access memory
RTC	real time clock
RSSI	received signal strength indicator
SSP	secure simple pairing
SM	security manager
SNR	signal to noise ratio
SPI	serial peripheral interface
QSPI	quadrature-serial peripheral interface
SAM	slot availability mask
SDM	SoftDevice manager
SDK	software development kit
SIG	special interest group
SD	super frame duration
SoC	system on chip
TDMA	time division multiple access
TPC	transmit power control

ULP	ultra-low power
URL	uniform resource locator
UART	universal-asynchronous receiver transmitter
USB	universal serial bus
VR	virtual reality
Wi-Fi	wireless fidelity
WLAN	wireless local area network
WPAN	wireless personal area network
WSN	wireless sensor networks

bps	bits per second
dBm	decibels
r	distance between receiver and interference node
d	distance between transmitter and receiver
GHz	gigahertz
I/O	input/output
Kbps	kilobits
Mbps	megabits
MHz	megahertz
m	meter
μA	microampere
mA	milliampere
mm	millimetre
ms	millisecond
mW	milliwatt
E	packet error rate
ppm	parts per million
Rx	receiver
Tx	transmitter
v	volt
W	watt
%	percentage
+/-	plus, or minus

1. INTRODUCTION

Communication has existed for ages. Wired as well as wireless communications – has been experienced in many forms as in early days smoke signals to communicate over distances and passing encoded messages to global positioning system (GPS) as well deep space communication in recent years. Nowadays, people are bounded with devices like cordless phones, smartcards, GPS units, wireless toys, sports equipment, satellite television, broadcast television, frequency modulation (FM) radios, headsets, remote controls, wireless keyboard, mobile phones and many more. Wireless communication delivers major assistance in high mobility environment such as high-speed railway system, compatibility with existing networks, convenient remote controls, zero setup time. Further, enhanced productivity, safety and security, connectivity in remote areas, reduced cost, highly reliable, equivalent or sometimes better speed than wired communication is possible with wireless technologies. Research possibility like satellite navigation, communication in remote, location-based optimized services as well deep space communication is possible with the concept of wireless communication. Among numerous wireless coverage technologies, body area network (BAN) and personal area network (PAN) concept provides various applications using technologies like Bluetooth [1], ZigBee [2], radio frequency identification (RFID) [2], near field communication (NFC) [2], adaptive network technology (ANT) [2], [3] etc.

Wireless technology has become vibrant part of our life that offers flexible choices based on the data rates and coverage. Bluetooth standard brings variety of ideas that is very much useful in making human life comfortable as well as eco-friendly. In the recent years, the use of the wireless sensor devices has been continuously enlarging, and with the concept of internet of things (IoT) [4], field specific applications will be developed in the coming years [1]. Some of the application field occupied by wireless sensor devices are medical and healthcare, smart home and factories, autonomous traffic, and environmental monitoring applications. Low-power wireless communication solutions are required by the IoT applications, as a sustainable operation of the devices are most for the operating environment. Some of the low-power technologies are Bluetooth low energy (BLE), and ZigBee [1]. Among them, Bluetooth stands out as the most commonly used in available commercial products. As the number of technologies are embracing the unlicensed industrial, scientific, and medical (ISM) 2.4 GHz band, the coexistence issue arises in the operating environment. So, the number of application scenarios need to be developed in such way that the performance of the devices does not degrade, and the communication is reliable. Especially for the medical and healthcare application, a developer must be aware of the issues related to the coexistence [2], [3], [5].

Bluetooth 5 was released in December, 2016 by Bluetooth special interest group (SIG). This thesis provides a comprehensive overview on Bluetooth technology and its development, coexistence issues and interference mitigation solutions and the performance of the Bluetooth 5 under interference. Particularly, two main technologies that operate at 2.4 GHz band: Bluetooth and ZigBee are considered. The experimental performance of BLE 5 [6] technique under interference is evaluated and results are introduced. The packet error rate (PER), and communication range performance of BLE 5 technique at different physical layer extension (PHY) modes under interference of ZigBee devices is evaluated. In addition, following conference paper has been published.

- H. Karvonen, K. Mikhaylov, D. Acharya, and M. Rahman (2018). "Performance Evaluation of Bluetooth Low Energy Technology under Interference", *13th EAI International Conference on Body Area Networks, At Oulu, Finland*.

This thesis is structured as follows. In Chapter 2, the importance of the Bluetooth standard, its development in different time frames, features associated with the different versions of Bluetooth technology, Bluetooth architecture, and competitive technologies in the 2.4 GHz band are presented. The protocol stack of low energy (LE) is presented in detail and more focus is given to the PHY and link layer (LL). Also, Bluetooth experimental range based on [7] is presented. Further, different changes that were made to BLE 5 as compared to BLE 4 in advertising extensions, improvement in frequency hopping (FH), PHY selection, and slot availability mask (SAM) are mentioned and finally significance of BLE 5 is presented.

The Chapter 3 presents the coexistence between different technologies in the 2.4 GHz band. Common wireless technologies and their coexistence mechanisms, interference avoidance approaches, channel overview of three most important technologies operating in 2.4 GHz: wireless fidelity (Wi-Fi), ZigBee, and BLE is presented. Finally, coexistence recommendations are presented for the sustainable communication.

In Chapter 4, devices used for measurement, functioning of advertiser and scanner, received signal strength indicator (RSSI) and packet layout are presented. A detailed overview on nRF52840 development kit (DK) [8], ZigBee, and S140 SoftDevice is enlisted with their important features, operations, and advantages. In chapter 5, experimental performance evaluation of BLE 5 technology is presented. The physical measurement location is discussed with the specification of the devices position and experimental procedures. Parameter setting for experimental performance is presented. Furthermore, the experimental results of the performance of BLE under interference scenario with PER vs BLE link distance is presented. The RSSI plot over link distance is presented. The advantages of coded mode are mentioned and comparison between BLE 4 and BLE 5 is presented.

In Chapters 6 and 7, discussion and difficulties faced while taking measurement is presented. Further, some ideas for Bluetooth technology to make it more sustainable in future. Reference and appendices are presented at the end.

2. BLUETOOTH TECHNOLOGY

Bluetooth was devised in 1994 and after that a series of updates has been made. Initially, Bluetooth 1.0, 1.0a and 1.0b objective was to replace serial cables with wireless link and faced many device operating errors at the protocol level. After that Bluetooth 1.1 was released in February, 2001 as institute of electrical and electronics engineer (IEEE) Std. 802.15.1 standard. This version fixed the previous versions errors and was able to define RSSI. In November 2003, with the launch of Bluetooth 1.2, adaptive frequency hopping (AFH) spread spectrum concept improves resistance to interference. Additionally, extended synchronous oriented (eSCO) links added to improve voice quality. This version provides faster connection as well discovery, higher transmission speeds up to 721 kbps. In 2004, Bluetooth 2.0 enhanced data rate (+EDR) was released which provides faster data transfer as bit rate of EDR was 2.1 Mbps. This provides more space for developers to define applications that required fast data. EDR uses Gaussian frequency shift keying (GFSK) and phase shift keying (PSK) modulation. Further, Bluetooth 2.1 +EDR released in 2007 which used a technique called secure simple pairing (SSP) that improves pairing of Bluetooth devices along with the securing while pairing. In basic rate (BR) and EDR, the frequency hopping (FH) rate is 1600 hops/s using 79 channels separated by 1MHz spacing. In 2009, Bluetooth 3.0 high speed (+ HS) was released providing theoretical data speed of 24 Mbps [1], [2]. Figure 1 list some of the most used consumer devices that is enabled with Bluetooth.

Figure 1. Different devices embedded with Bluetooth technology.

The main feature defined by v3.0 was an alternative MAC/PHY access for transporting Bluetooth profile data. This feature is still in use for discovery, initial connection and configuration. The main concept was to make connection using Bluetooth and moving on to 802.11 chip to achieve high data transfers. The Bluetooth 4.0 specification defines BLE and extends the low power feature further. Star topology was introduced. In Bluetooth 4.1, master and slave concept was introduced. A slave can be connected to several piconets [2]. This expands the topology option in this version. Some of the highlighted features are logical link control and adaptation layer protocol (L2CAP), connection oriented, limited discovery time, and dual mode topology. In Bluetooth 4.2, the throughput, internet connectivity and security are improved. Some of the features of BLE series can be summarizes as ultra-low power (ULP), low cost, small size, fast connection (link setup time reduced to 3 ms), secure connection, interoperable. In BLE 5, range, advertising channel functionality and, data rate are much improved as compared to BLE. The maximum output signal power ranges from 1 mW to 100 mW [1], [2].

As the success of IoT is rising, the number of connecting devices to the internet is in successive progressions. In 1990s, the number of the devices connected to the internet were approximately 1 billion. As the smartphone were introduced, devices connected to internet were 2 billion in 2000s. As the concept of IoT arises, the predicted number of connected devices to the internet will be 48 billion by the end of 2021 and, 30% of the smart devices connected to internet will include Bluetooth technology [6], [9].

The key features of Bluetooth technology are low power consumption, robustness, and low cost. Bluetooth technology comes in different versions from “Classic” to “LE” and now ‘Bluetooth 5’ [2]. All these versions include device discovery, connection establishment and connection mechanisms. The basic rate (BR) system includes alternate MAC, PHY and optional enhanced data rate (EDR). The BR and EDR system offers synchronous and asynchronous connections with data rates of 721.2 kbps and 2.1 Mbps respectively. The LE enables products with low power consumption, lower cost and low complexity as compare to BR or EDR. So, LE design is applicable to the applications with lower duty cycle and low rate requirements. Similarly, the range of the applications it includes has been broadened. Bluetooth is able to provide wireless keyboards, headsets and, speakers. In addition to those applications, recent Bluetooth technology can serve areas like health care and fitness [10], [11] .

Research and development has been carried out continuously, so that standardisation of products, adoption and acceptance worldwide and, interoperation of products from industries to consumer is maintained. SIG reserve all the rights related to Bluetooth and do tasks like protecting the Bluetooth trademark, publish Bluetooth specifications, and govern the qualification program for the quality development [3].

BLE is convenient for low-power, short-range, low-cost wireless applications. Initially Bluetooth was originated as cable replacement technology but over the years embedded in almost every electronics consumer product like headsets, gaming consoles, car kits and many more.

Bluetooth SIG has outlined the capability of Bluetooth 5 is to provide 4 times range, 2 times speed and 8 times broadcasting message capacity with increased functionality to provide the reliable IoT connections [11]. BLE 5 shows stronger robustness to interferences as compared to BLE 4 results in improved coexistence with other wireless technologies and interoperability [6].

Bluetooth operates in the 2.4 GHz ISM band and the frequency range is 2400 – 2483.5 MHz. Power levels at the antenna connector of the Bluetooth devices has been defined in three different classes. At 0 dBm, 4 dBm, and 20 dBm transmission power the maximum power outputs are 1 mW, 2.5 mW and 100 mW. The modulation is GFSK with a bandwidth-bit period of BT = 0.5. The binary one is represented by a positive frequency deviation, and binary zero is represented by negative frequency deviation. The reference sensitivity level referred in the Bluetooth device is -70 dBm. The sensitivity level of the device is defined as the input level for which a raw bit error rate (BER) of 0.1% is met [10]. The newest specification defined by the Bluetooth SIG for the BLE 5, together with its first official specification for mesh topology is drawing so much attention. Additionally, with stronger robustness and mesh topology features, devices equipped with Bluetooth 5 can now transfer information faster with stable connection [5].

For data security, Bluetooth has 8-128 bits (configurable) for Encryption key and 128 bits key for Authentication type. Both BLE and BLE 5 finds a wide variety of applications such as IoT, proximity and presence sensing, advertisements, mobile payments, security, home automation, home entertainment, remote controls, smart energy, sports and fitness equipment, health care devices, automotive kits and many more. Bluetooth technology allows devices to communicate with each other through radio links with low power, low cost and short-range applications. Nowadays, most of the devices are embedded with Bluetooth. Bluetooth is widely used in gaming consoles, mouse, printers, scanner, headphones, car kits, sports kits, health kits and several more that are supporting wireless technology.

Wireless personal area network (WPAN) technology includes Bluetooth and other technologies like universal serial bus (USB), ZigBee, and NFC. The most implemented version, BLE technology focuses on reducing both the peak current and the average current which results in low power consumption and coin cell batteries physically. BR supports devices to a maximum data rate 721Kbps. BLE specification defines 40 frequency channels for FH. Each channel has 2 MHz bandwidth, out of 40 channels 3 channels are used for the advertising and other 37 data channels. BLE follows frequency hopping spread Spectrum (FHSS), which changes transmission channel after every connection event (CE). This concept advantage Bluetooth to blacklist the channels with low quality. In this way BLE avoid highly interfering channels [2], [3].

2.1. Bluetooth low energy (BLE) protocol stack

Bluetooth product can implement one or more core configurations, in compliance to the required parts of the specifications, fulfilling the mandatory requirements. The different radio frequency (RF) stages of the devices are standby, advertising, scanning, initiating and connected. The RF states are controlled by generic access profile (GAP). The device which initiate the connection will be master and the one which accept the request becomes the slave. Advertiser function is to transmit data no matter the device is connected or not, but scanners are the one to scan advertiser and connection state is only achieved when an initiator responds to the advertiser with request [3].

Bluetooth is a full protocol stack as shown in Figure 2 [10]. The BLE protocol stack consists up of controller and host which are implemented separately. Some of the features supported by the protocol stack are slave feature exchange, connection parameter request, 2 Mbps PHY for LE, channel selection, secure connection, L2CAP connection-oriented channel support, and data length extension.

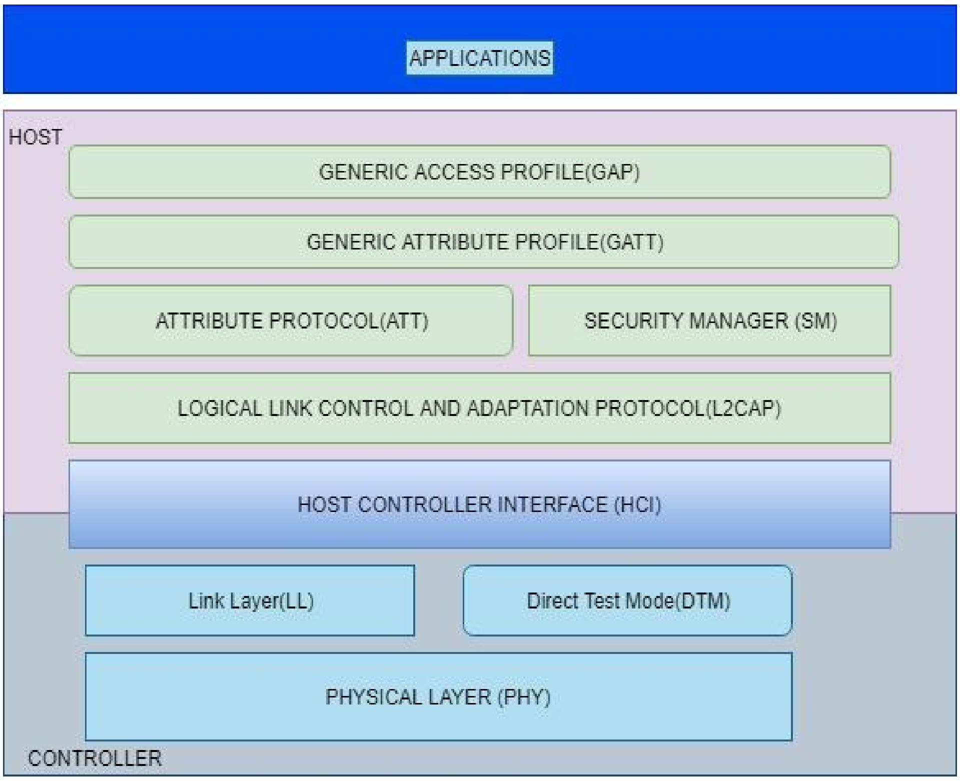

Figure 2. BLE protocol stack.

As shown in Figure 2, the host controller interface (HCI) provides communication between the controller and the host. Host executes the upper layer of the Bluetooth along with profiles and Bluetooth applications. The host software executes on a microcontroller or application processor. Lower layer of the Bluetooth is executed by the controllers which contains layers radio link manager and Baseband. The HCI facilitate communication between Host and the Controller. HCI may run using RS-232, USB, or universal asynchronous receiver-transmitter (UART). HCI also ensures vendors compatibility with the devices [3], [10].

To provide end-to-end communication of the data, the L2CAP provides data encapsulation service. The security manager (SM) ensures the securely connection and exchange of data between devices by defining the pairing and key distribution. The GAP handle device discovery and connection related services along with the initiation of the security. Attribute protocol (ATT) layer exposes certain pieces of data from one device to another device. The GAP define rules for using ATT, so GAP act as service framework [10].

Each controller defines own clock which starts when device is powered on. Bluetooth clock help in synchronize with other peripheral devices, the clock offset values are used for synchronization as each device have a different absolute value of clock. Crystal Oscillators drive the Bluetooth clocks with +/- 20 ppm (parts per million), which means the clock cannot drift more than 20 ticks in a million ticks compared with fully accurate reference clock. The real time clock (RTC) of daily life use runs even system is off but Bluetooth clock starts with power on, this differentiate normal clock with Bluetooth clock. When exchanging the data packets between the devices, the device must follow certain protocols defined by protocol data unit. Some example of packet data unit (PDU) are Packets sent by upper layer (e.g. L2CAP) to corresponding upper layer of the peer Bluetooth device [1].

2.2. The physical layer

The bottom layer is referred as PHY. The PHY layer is responsible for transmitting and receiving signals on the physical channel. A control path between PHY layer and baseband is established to allow the baseband block to control the timing and frequency carrier of the PHY layer. It determines how a bit and its values are represented over the air. So, from a physical channel, PHY layer transforms a stream of data into required formats [10]. Different PHY specification has been defined to the different versions of Bluetooth. In comparison to the Bluetooth 4, Bluetooth 5 adds two new PHY variant. The PHY can be named as LE 1M, LE 2M, and LE coded [6], [12].

The BLE 4 uses GFSK modulation scheme and utilize LE 1M PHY with a data rate of 1Mbps. The LE 2M operate at 2Mbps. As compared to LE 1M, LE 2M could transmit data with the reduced amount of the airtime results in greater spectral efficiency. Two level GFSK is used in LE 2M where binary zero represent decrement of carrier frequency by a given frequency deviation and binary one represents increased carrier frequency. The frequency deviation used by LE 1M is minimum 185 kHz and LE 2M PHY is 370 kHz minimum. By switching the PHY, the physical properties of the RF signal is changed. The LE coded PHY shows improvement in the range as compared to BLE at the same transmission power. This is accomplished by coding the signal, so that the transmission power remains same. This means the power consumption per time stays the same. Alternatively, coding entails the lower data throughput.

2.3. The physical layer (PHY) selection

The use of new LE coded PHY mode shows the capability for “long range” applications as compared to the LE mode. . Table 1 enlist all the PHY mode features in the Bluetooth operation.

Table 1. Key PHY features in Bluetooth 5

	LE 1M	**LE 2M**	**LE Coded (S=2)**	**LE Coded (S=8)**
Symbol rate (Ms/s)	1	2	1	1
Range multiplier	1	0.8	2	4
Error correction	None	None	FEC	FEC
Error detection	CRC	CRC	CRC	CRC
Data rate	1 Mbps	2Mbps	500 kbps	125 kbps

The HCI supports changing of the PHY mode as per the application requirement. For each transmission or receiving of data HCI command cab change the PHY procedure so that the required data rate transmission is achieved by switching the mode of transmission [9]. So, now it is easy to switch to “long range mode” or “high data rate mode” or “low data rate mode” depending on the application requirement and, communicating environment BLE provides applications which involve small data rate but are unable to provide low-power wireless applications with higher data rate than its limit. BLE seems unable to fulfil the multiple dimensions of the measurements such as that needs to be find for the higher accuracy of the applications, for example, human physiological data. So, especially in the medical field the LE 1M was not enough [9].

2.4. Link layer (LL) and states

The LL is responsible for the creation, modification and release of logical links, as well as the upgrade of parameters associated to physical links between the operating devices. LL protocol communicate with remote device so as to make updates. As LL directly interfaces to the PHY layer, it is responsible for the advertising, scanning and maintaining connections between Master and Slave devices. The Bluetooth LL in terms of state diagram is presented in Figure 3. LL state machine allows only one state to be active at a time and LL may have multiple instances of LL state machine. One state machine supports one of the advertising states or scanning state [1], [2].

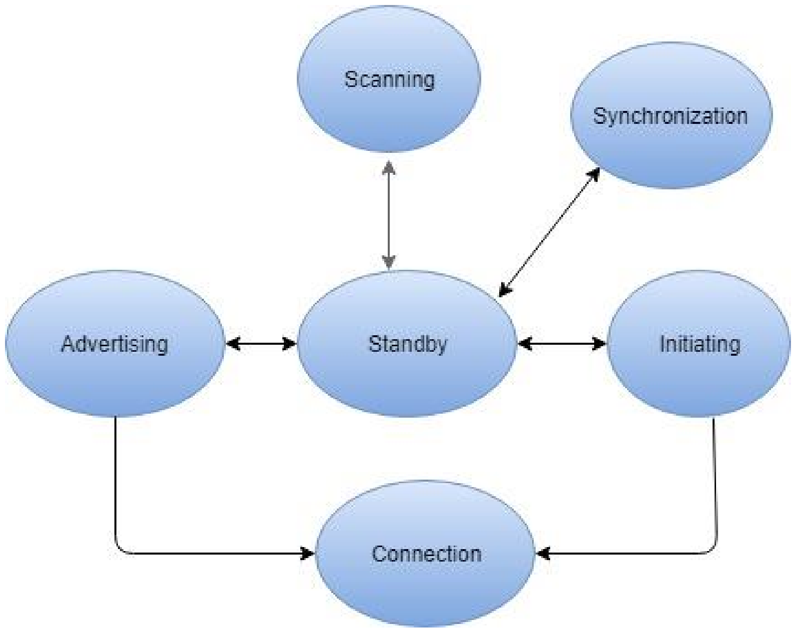

Figure 3. Bluetooth LL states.

A BLE mode where there is no transmission or reception of packets is referred to be Standby state and this state might occur anytime from any other states except connection state. When the LL acknowledges advertising physical packets from a specific BLE device then the Initiation state will start. Initiating state responds to the advertising packets to initiate a connection from another device. Advertising state can be reached from the Standby state when LL will transmit advertising packets and wait for the responses from another Bluetooth device. In Scanning state, LL listens for advertising packets from another advertising device. A Connection state can be reached from “Advertising state” or “Initiating state”. A Bluetooth device is either Master or Slave. If Connection state is entered from “Advertising state” then it will be in Slave role and when from “Initiating state” it will act as Master. As Master role, LL will communicate with the device to become Slave role and define the transmission time. A Synchronization state can be entered from “Standby state”. Periodic channel allows specified device to transmit periodic advertising which occurs in Synchronization state [1], [10].

2.5. Bluetooth range

The maximum range occupied by any communication technology refers the maximum distance at which the receiver can process the received signal correctly. The message bits is modulated by a carrier signal. At the receiver side, the receiver must decode the received signal properly and turn the signal back in the message bits. So, the receiver task is always complicated by the background noise in the environment. If the power level of the interference is equal to received signal power, the decoding process will be more complicated. So, technically the ratio of the signal power to noise power is termed as signal to noise ratio (SNR). The strength of the receive signal is totally dependent on the distance between transmitter and receiver, more the distance weaker the received signal. BER measures the level of errors and shows the probability that the transmitted bit will be incorrectly decoded by the receiver [2].

The summary of measurement results from [7] are presented below in Table 2 with different PHY modes in line-of-sight (LOS) and non-line-of-sight (NLOS) scenarios.

Table 2. Measurement results from [7]

Mode	Tx Power (dBm)	Range (m)	Max Throughput (kbps)
Indoor scenario			
BLE 4	0	43	262
BLE 5	0	48	26
BLE 5	9	51	26
Outdoor NLOS scenario			
BLE 4	0	90	262
BLE 5	0	123	26
BLE 4	9	138	262
BLE 5	9	165	26
Outdoor LOS scenario			
BLE 4	0	220	262
BLE 5	0	490	26
BLE 4	9	430	262
BLE 5	9	780	26

As per the marketing material advertised by the Bluetooth SIG, the Bluetooth 5 coded version allows range to be quadrupled compared to BLE without increase in the transmission power required. The measurement data shows that practically it is not 4 times, but the range improvement shown by Bluetooth 5 is appreciable. The 9 dBm gain improvement by Bluetooth 5 coded as compared to BLE conclude that the similar performance of BLE can be achieved by lowering 9dBm transmit power with Bluetooth 5 coded mode. At 9dBm, the range occupied by Bluetooth 5 was found to be 780 meters, which is closer to targeted 4-fold improvement as compared to BLE 4 range with 0 dBm. For both modes, with the same transmission power, we can conclude that in indoor scenario, the range improvement has found to be around 10-20 %. For NLOS scenario, 20-37% improvement is noticed [7].

2.6. Bluetooth 5 advertising extensions

As compared to the Bluetooth 4, some significant changes has been made in Bluetooth 5 in how advertising may be accomplished. 37 octets long advertising packets were used in BLE 4 with a 6-octet long header and payload of maximum 31 octets. Among 40 channels, three dedicated channels 37, 38, and 39 as shown in Figure 4 has been used for the transmission of advertising packets. The total 40 channels are numbered from 0 to 39, with each channel being 2 MHz wide. In Bluetooth 5, 8 new PDUs have been added to GAP for advertising, scanning, and connection purpose. The 8 new PDUs [9] allows advertising to be executed in a deterministic behaviour, multiple distinct sets of advertising data to be broadcast, and most importantly larger amounts of data to be broadcast in connectionless environment.

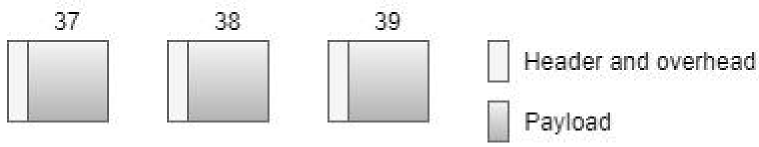

Figure 4. Advertising and channel usage in BLE 4.

Bluetooth 5 is a promising technology for developing next-generation beacon products and allow heterogeneous, much richer sets of circumstantial data to be distributed by beacons rather than just a uniform resource locator (URL) or identification (ID). As shown in Figure 5, Bluetooth 5 permits packets up to 255 octets long through offloading the payload to one of the channels among 0-36 numbered channel range, while in preceding Bluetooth only one channel was used for the CE. A CE is the time slot during which data is transmitted over the connection. The AuxPtr [10] containing advertising payload is transmitted on a secondary channel which includes the channel number so that receivers know the transmitted data sequence [9], [13].

Figure 5. Bluetooth 5 larger advertising packets and channel offload.

Further, for the transmission of larger amount of data Bluetooth 5 allows the advertising packets changing as shown in Figure 6, where packets are chained together, and different subsets of a whole data set is maintained. Each chained packet contains an AuxPtr header field which references the next in the chain.

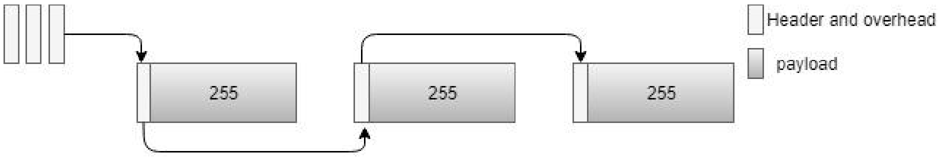

Figure 6. Advertising packet changing.

Furthermore, Bluetooth 5 introduces a mechanism for the advertising payload to vary, so several, well defined sets of advertising data is feasible. Each advertising packet clarify its own parameters and a distinct ID attached to each advertising set make belonging packets distinct. An advertising sets may use primary or the secondary channels so the task of transmitting and scheduling the different sets now falls to the LL in the Controller rather than having driven by the Host. This makes Bluetooth 5 more power efficient [10], [11].

In Bluetooth 5, periodic and deterministic advertising is possible so that synchronization of the scanning packets is much efficient for the scanner. The scanning is more power efficient than before and most importantly the uses of Bluetooth in the connectionless scenarios is more effective [9], [12]. Whereas on the other side, in Bluetooth 5 random delays were inserted in the advertising event scheduling process. So, the GAP defines synchronized and a non-synchronized mode. In synchronized mode, a periodic advertising synchronization establishment procedure is defined.

Furthermore, one of the most important changes in the Bluetooth 5 is now the secondary channels numbered from 0 to 36 are carrying most of the heavy data traffic while the primary advertising channels 37, 38, and 39 are carrying less data [10]. Now, only small headers are occupying the primary channels and advertising data using all available channels, there is less contention on the channels. Same payload transmit process in Bluetooth 4 and Bluetooth 5 is different. In Bluetooth 4 as shown in Figure 7(a), payload transmits was up to three times on three different channels. On the other side, Bluetooth 5 as in Figure 7(b), now transmits such data only once, with small headers referencing it from the primary channels.

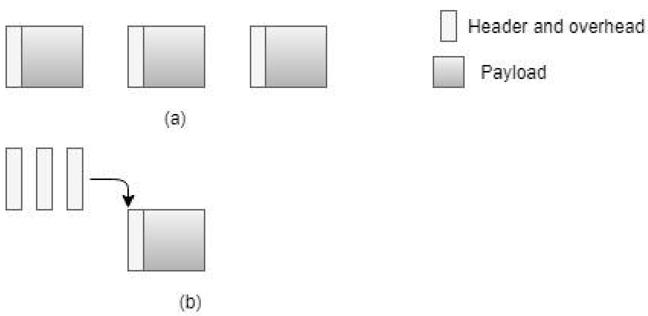

Figure 7. Reduced contention and duty cycle. (a) Bluetooth 4 repeating the payload on channels 37, 38, and 39 (b) Bluetooth 5 transmitting the payload only once on a secondary channel.

In this way, the total amount of overhead is less and hence, duty cycle has been reduced. The minimum advertising interval has been reduced to 20 ms in Bluetooth 5 from 100 ms in Bluetooth 4 for non-connectable advertising. This will result in rapid recognition and responses to advertising packets in the upcoming devices [10].

The Extended Advertisements along with Periodic Advertisements is a useful feature of Bluetooth 5. As Beacons are capable of broadcasting more data, a better user experience is accomplished. Also, the connectable devices can concede connections on the secondary channels, which is worthwhile to avoid interference and noise from other devices broadcasting on the primary channels [12].

The Periodic Advertisements are used for broadcasting packets to devices at a specified period between two unconnected devices. A scanner can target an advertising device by first discovering the advertisement event on the primary channel, and then tuning the appropriate secondary channel and timing based on information sent in the primary advertisement packet. The exercising of Periodic Advertisements also assists in adjusting the broadcasting device more incessantly discovered and monitored.

Aiming at the improved performance on broadcasting various advertising PDUs has been added to BLE 5. The PDUs let two unsynchronized Bluetooth devices to interchange data and eradicate the need for pairing when broadcasting. Therefore, the efficiency for the receiving beacons is significantly improved, and connectionless advertising can be comprehended.

2.7. Frequency hopping

FHSS technique transmits the information by “hopping” the signal across several different frequency channels according to a predetermined sequence. On the receiver side, the receiving of the information signal is on the same frequencies using the same frequency hopping sequence. The radio communication process is a step-by-step process on the defined period and radio channels, where the frequency hop channel numbers are sanctioned to receivers. Since the Bluetooth standard is working in ISM band, there is a high possibility for interference with other working devices in the same frequency band [1], [2].

AFH determines the radio channel to transmit and receive data by selecting the proper channel so that data is transmitted over a wide selection of channels. Bluetooth device makes it possible for communication with other devices by deciding which channel to use from the available 37 data channels during communication. AFH continuously monitor the communication environment by determining the interference scenario and continuously changing the common channel map according to the interference. The basic idea of AFH is to periodically change the channel frequency shared by each member of a piconet. AFH can reduce the effects of the interference between the Bluetooth and other types of devices operating in the same environment. AFH adapts the access channel sharing method, which does not allow the transmission of information from the channels that have significant interference. This is how Bluetooth performs well in dense networks environment. The interference avoidance characterises help to detect the devices that are operating within the same frequency band and within the same physical area. After detection, the AFH reassigns the transmission of packets on the frequency channels that have lesser interference levels so that the cross interference caused by each other is reduced. The reduced in interference increases the amount of successful transmissions. In this way the overall data transmission rate as well as efficiency of the Bluetooth device is increased.

The channel map updating procedure is a continuous process and an important part of Bluetooth 4 specification. A channel map is the exchange between the master and slave devices. The peer devices decide which channel to use among 37 data channels with the help of channel map so that the communication process is continuous. The channel map procedure is initiated by the master only. Since the channel map update procedure is adaptive in nature, it is easy for a Bluetooth device to block low-quality channels dynamically and make device operation more reliable.

BLE defines two kinds of channel selection algorithm. Algorithm#1 [10], [13], [14], [15] is mandatory to support in which channels are selected sequentially using fixed hop interval during the connection establishment. The BLE channel selection algorithm#1 is presented in Table 3. In Algorithm#1, bleChannelSelection defines a new channel index. The system object configures the field required for selecting a channel index. Now, the fields are configured as follows, the HopIncrement property defines the hop increment count to be used. The default value is 5. This property is applicable for Algorithm #1. The UsedChannels property defines the list of used (good) data channels.

ChannelIndex is a read-only property that indicates the current channel being used. EventCounter is a read-only property that indicates the number of connection events occurred until now. It is incremented for every new selected channel. For selecting a channel index for next hop object csa is called as a function to determine next channel hop and to select new channel for each connection event. As an output, the selected channel will be 9 for connection event 1 when using 'Algorithm #1'.

Table 3. Channel selection algorithm#1

Channel Selection Algorithm#1	

System object	csa=bleChannelSelection ('Algorithm', 1);
	csa.HopIncrement =8;
	csa.UsedChannels = [0, 5, 9, 13, 24, 36];

BLE channel selection properties	Algorithm: 1 HopIncrement: 8 UsedChannels: [0 5 9 13 24 36] ChannelIndex: 0 EventCounter: 0
Channel update	nextChannel = csa() fprint ('the selected channel will be %d for connection event %d when using 'Algorithm #1' : nextChannel, csa.EventCounter)

In algorithm #2 [10], [13], [14], [15] the channel to be used is calculated from current event counter and access address and the selected channel is semi-random in nature. The remapping algorithm is used to remap the channel, if the usable channel is blocked on the common channel map. The BLE channel selection algorithm#2 is presented in Table 4. In Algorithm#2, the access address property defines the 32-bit unique connection address between the devices. The default value is 'E89BED68'. The UsedChannels property defines the list of used (good) data channels. To determine next channel hop and to select new channel for each connection event object csa is called as a function. As an output, the selected channel will be 21 for connection event 1 when using ‘Algorithm #2’.

Table 4. Channel selection algorithm#2

Channel Selection Algorithm#2	
System object	csa = bleChannelSelection (‘Algorithm’, 2); csa.AccessAddress = ‘E89BED68’; csa.UsedChannels = [9, 10, 21, 22, 23, 33, 34, 35, 36];
BLE channel selection properties	Algorithm: 2 AccessAddress: ‘E89BED68’ UsedChannels: [9 10 21 22 23 33 34 35 36] ChannelIndex: 0 EventCounter: 0
Channel update	nextChannel = csa() fprint (‘the selected channel will be %d for connection event %d when using ‘Algorithm #2’ : nextChannel, csa.EventCounter)

In Bluetooth 4, the channel selection algorithm used in frequency hopping produced only 12 distinct sequences of channel and all packets in a given CE would use the same channel, which is not an optimized approach for some applications, such as audio.

In Bluetooth 5, a new channel selection algorithm is introduced, in which hopping sequences are pseudo random in nature and the distinct sequences are very large. Channel selection algorithm uses shared event counter, which ensures that each peer in the connection selects the same channel from next available channel in pseudo-random sequence. Bluetooth 5 adopts the above-mentioned algorithm #2. The hopping algorithm used is chosen by the master at connection time [13].

2.8. Interference detection and slot availability mask (SAM)

As the AFH procedure is enabled in Bluetooth device, at least one connection is active or at least one advertiser is running with extended advertisements. In the meantime, the Bluetooth protocol stack runs periodically in the background which sweeps all the channels based on the scan intervals and measured received power on each channel. Here, if the measured received power is beyond -71 dBm on a channel, then the channel is blocked for 8 scan intervals. If interference is still found on the channel, unblocking that channel needs 8 consecutive measurements with no interference detected. After this one sweep cycle, the common channel map is updated and become new channel map. The new channel is updated based on the interference, after which the master device sends the channel map to all slaves. Slaves cannot initiate the channel map update. The sweep of 40 channels takes around 10 ms and the scan interval is 1 second by default. The scan interval can be changed at any time depending on the requirement of radio operation of the Bluetooth stack [16].

Bluetooth 5 has introduced a system called SAM, to help to improve the coexistence with other radio technologies. SAM allows Bluetooth to indicate the availability of its time slots and to synchronize in an optimal manner with the help of mobile wireless standard (MWS) bands [9]. From the baseband point of view, SAM provides a map called SAM slot map, which marks the availability of Bluetooth slots. The availability arises from either external condition or internal condition. For example, MWS coexistence can be external condition, and topology management for scatter nets can be internal condition. With the SAM slot map availability of Bluetooth slot is shared, this enable the control of data sharing and receiving on the Bluetooth slots.

2.9. Bluetooth mesh

Mesh topology allows redundant interconnections between network nodes. Bluetooth networks has suffered long from short coverage and lack of extensibility. With mesh, massive connections is possible with range extension. The IoT based applications first priority will be the ubiquitous connectivity among the surrounding devices. Many technologies are competing with each other's to fulfil this goal, but none of them can fit into all application scenarios. So, other technologies such as Z-Wave and IEEE Std. 802.15.4 based technologies like Thread and ZigBee are also supporting mesh topology. After the release of BLE 5, Bluetooth SIG has released new specification on network topology as Bluetooth Mesh. The combination of the Bluetooth Mesh topology and BLE 5 has brings alternations and opportunity in order to provide complete solutions to meet the demands of seamless communications in the IoT era [5], [15].

Mesh networks enable many to many relation between nodes, which means that each node in a network can communicate with every other nodes using multiple-hop communication and path diversity [17]. Figure 8 illustrates three basic network topologies, where communication between two devices to many-to-many devices is shown.

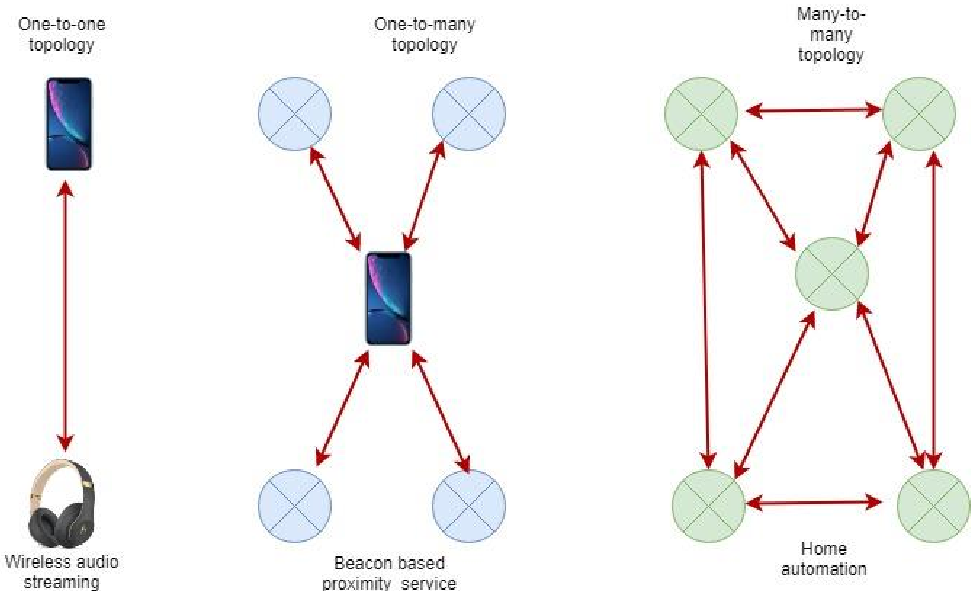

Figure 8. Three examples of different topologies of Bluetooth.

In mesh topology [17], each Bluetooth device is called as a node and nodes of Bluetooth mesh networks communicate with each other through messages in an advertising manner as shown in Figure 9.

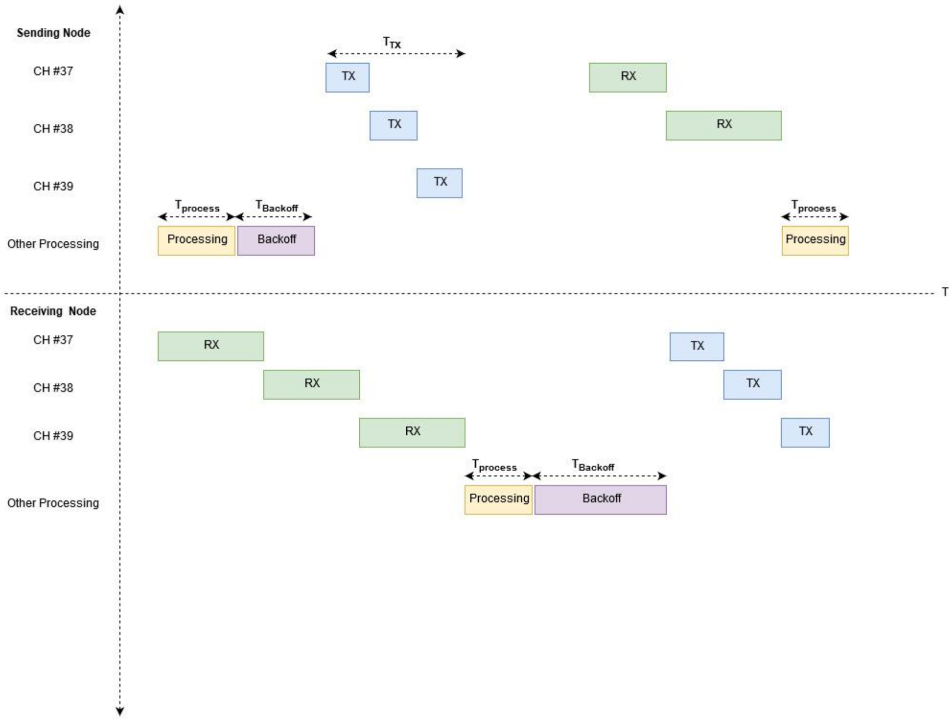

Figure 9. Communication between two nodes in a Bluetooth mesh network.

Initially, an event on the application layer of the sending node (pressing a PHY option) triggers the need to send message to another node. It takes some processing time for that message to be sent from top to bottom in the stack. Before the message is sent over the air, a random Back-off mechanism is used that holds the message for a random time between 0 ms and T_{max} (configurable). Ultimately, the Back-off expires and the message is broadcasted. Altogether a message is advertised on channels 37, 38, and 39 sequentially and a receiving node is scanning on one of these channels, switching form one channel to another channel at a fixed interval. The message is sent on three advertising channels. The time required to send a message on one channel depends on the size of the packet and the configured bit rate of the BLE radio [17]. A message will contain the address of the sender node and its intended receiver node and some other controls fields. The address is included in messages so that the device will be acknowledged communication is reliable. Provisioning is the process of adding one Bluetooth device to the mesh network. Five stages are defined for the adding procedure: Beaconing, invitation, exchanging public keys, authentication, and spreading of the provisioning data [5]. The other node is scanning on the packets and depending on the channel utilized during the transmission of the packet, the node takes a definite time until the packet is being received.

2.10. The significance of Bluetooth

Bluetooth wireless technology is put up into many products, from mobile phones, to the complex medical devices and the computers to share the data among paired devices. This interoperability standard potentials to transfigure the scope to practice smart connected products and compatibility between the devices now and in the future. As every smartphone, tablet, and current wireless devices are assimilated with BLE, Bluetooth exploration has conquered all other standards challenging for the dominance in the IoT world. Due to power efficiency feature, a Bluetooth device can function for years without having need to refresh the power source as the operating power of Bluetooth is low [2], [6], [9], [15].

The main features of Bluetooth 5 and the required data rate are presented in Table 5. According to the advertising document from Bluetooth SIG, the range improvement in Bluetooth 5 is 4 times than that of BLE, on-air data rate is double than BLE, up to 2Mbps from 1Mbps in BLE and eight times the broadcasting capacity as compared to BLE [9].

Table 5. Bluetooth 5 highlights

Bluetooth 5 data rates	2 Mbps (new)	High throughput
	1 Mbps	Bluetooth LE data rate
	500 kbps (new)	Longer range
	125 kbps (new)	Longest range

The long-range feature introduces by the Bluetooth 5 provides a basis for achieving robust communication for the smart home and medical application. Further, advanced wearable such as connected health and personal fitness applications are also benefitted. Interactive entertainment devices such as gaming controllers, virtual reality (VR) applications and advances remote control applications are in full swing. Another important field that Bluetooth 5 feature covers is IoT concept, which is promising technology for the huge number of applications in the coming years.

Bluetooth 5 is permitting development of pioneering designs in less space with full flexibility. The LE 2M provides higher symbol rate and hence, improves the spectral efficiency. Due to this, a range of application development is possible. For example, from home automation concept to sports and medical equipment devices. Bluetooth 5 advertising extension is a promising concept to fulfil the next-generation beacons, IoT applications as well as advanced audio applications and more. Many industrial applications, remote control applications, health and medical devices, gaming controls, smart home concepts will be fulfilled with the concepts of Bluetooth 5. Based on three different topologies various applications based on Bluetooth technology can be drawn, and they are discussed below

One direct benefit of Bluetooth technology is more powerful communication link for paired devices. For applications using Bluetooth to perform one-to-one communication, with Bluetooth 5, one can enjoy either faster speed or longer range while keeping performance quality uninfluenced. Beacon-based proximity detection is one practical example for one-to-many topology, where beacon device continuously broadcast their IDs and contained information to neighbour devices. End device then collect multiple IDs for localization based on distance or angle to the beacon device.

In Many-to-Many or meshed topology, BLE 5 extends applications such as smart home or offices and industrial controls IoT scenarios that supports many-to-many device communication [13], [16].

2.11. Competitive technologies

Based on the functional requirement, every technology bear advantages and disadvantages from the technical as well commercial perspective. Bluetooth technology is competing in the same space with many other technologies and some of them are detailed below

- ZigBee: This 2.4 GHz radio frequency standard feed low-power, low-cost wireless applications and is easy to implement. Many Industrial, government, business, consumer user applications are using ZigBee wireless performance. Variety of innovations has been designed on ZigBee base which are cheaper and environment friendly.
- NFC: This technology is useful for consumer's application like exchanging digital content, and connecting electronic devices. This contactless technology provides solutions to various application field related to transport, loyalty, payments, health care, access control, consumer electronics, information gathering and exchange. Some of the benefits of NFC [5] are versatile, inherently secure, technology-enabling, interoperable and intuitive.
- ANT and ANT+: This ULP standard is flexible technology that wirelessly send information between devices in robust manner. ANT suited to applications with low data rate technologies as well as PANs applications like sports, fitness, and wellness and home applications. ANT is easy to implement with low-cost, network adaptive, resource optimized and ULP [5].

Communication technologies are proposed to fulfil the requirements of certain applications. For example, ZigBee was proposed for enabling low-power and networked devices, classic Bluetooth for providing short range communication. As the technology become crucial with time, many updates were made with improved performance and new features. Table 6 presents three different technologies and their features [5].

Table 6. Comparison among BLE, ZigBee, and Wi-Fi

Technology		**BLE 4**	**BLE 5**	**ZigBee**	**Wi-Fi**
Speed (maximum data rate)		1 Mbps	2 Mbps	250 kbps	600 Mbps
Energy efficiency (battery life)		High	High	High	Low
Network capacity (maximum number of nodes)		8	32,767	>65,000	255
Coverage	mesh support	No	Yes	Yes	No
	indoor transmission range	10-20 m	40 m	10 m	<50 m
Accessibility (exist in cell phone)		Yes	Yes	No	Yes

3. COEXISTENCE

The ISM radio licence-free band is utilized by the number of radio applications such as Bluetooth, WLAN, ZigBee, etc. The equipment using these technologies must share the same spectrum. ISM band coexistence achievement targets to sustain acceptable performance of the devices in the presence of interference from the operation of other devices sharing the same band, and to minimize the generated interference between the devices so that other device sharing the same band can also have acceptable performance [5], [18]. In the coming years, the number of wireless devices utilizing the ISM band will increase dramatically [2], [12]. The wireless devices operate under defined radio spectrums and distributed by electromagnetic radiation or other sources. Fundamentally, the terminals must operate in specified bands but conflicts between various operating applications may impact the performance, for example wireless local area network (WLAN) and Bluetooth operates in the same band and they could be interference to each other if they operate in the same frequency band.

Figure 10 lists some of the wireless technologies operating at 2.4 GHz band. It is apparent that due to large variety of technologies, the ISM band is crowded. Among these technologies, BLE is found in majority of commercially available devices [19]. Different wireless technologies need to be complimentary with each other rather than opposing so that the generated applications is desirable and hence there is no degradation in each other's performance. So, it is very necessary to understand

- How these various technologies can coexist within the same band?
- How each technology is impacting each other's performance? And, if there is any impact, how it can be minimized?

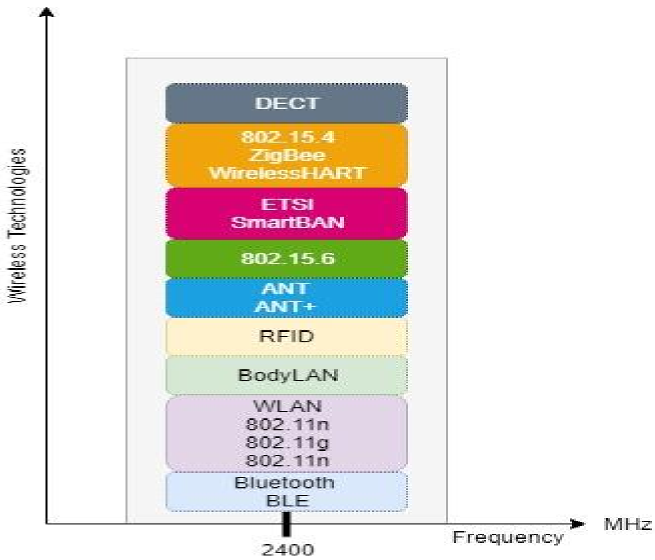

Figure 10. Common wireless techniques at 2.4 GHz ISM band.

WLAN standard wireless devices and infrastructure have been widely deployed in business offices, campuses, airports, and in households. In every portable devices, Bluetooth has become an integral part requiring short range communication. The performance of the devices under Bluetooth technology in various environmental conditions must be measured in terms of the transmission latency, data throughput, or both. In terms of the coexistence issue, evaluating the performance requirements help to define the device qualification for the interference susceptibility and usage policies [20].

In the communication process between transmitter and receiver, the interference phenomenon can affect the quality of message signal. In case of the transmitter (Tx) transmitting to receiver (Rx) as shown in Figure 11(a), when the source is located away from the interferer, interference comes out as collision between two communicating devices. For example, when the IEEE Std. 802.11 source is located far away from IEEE Std. 802.15.4 interferer, interference comes out collision between IEEE Std. 802.11 and IEEE Std. 802.15.4 data packets. In case of Transmitter transmitting to Receiver as shown in Figure 11(b), when source is located close to the interferer, interference results in channel occupation between two communicating devices [20]. For example, when the IEEE Std. 802.11 source is located closely to IEEE Std. 802.15.4 interferer, interference comes out as channel occupation due to the presence of IEEE Std. 802.15.4 emissions in the IEEE Std. 802.11 channel. An ideal channel occupation is the state when the transmitter node can transmit data without interfering the other node.

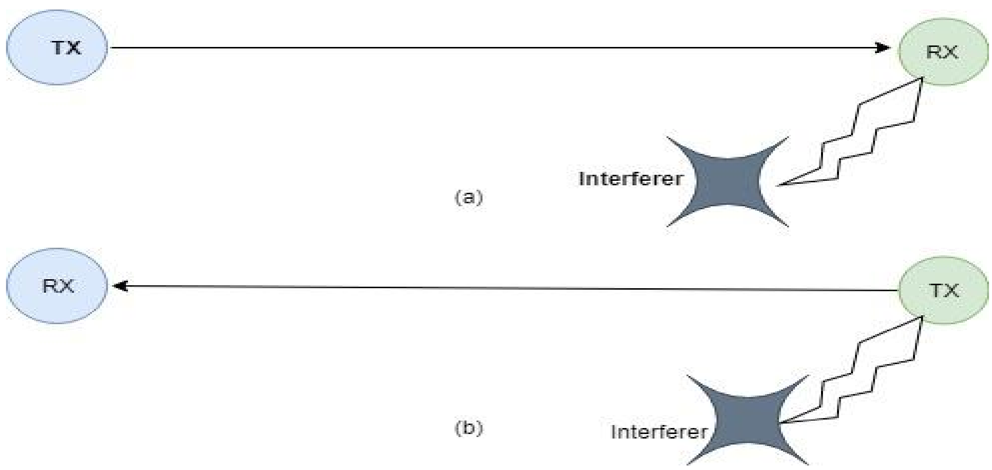

Figure 11. Interference on receiver and sender- (a) collision, (b) channel occupation.

The widely deployed Bluetooth technology and other technologies such as Wi-Fi and ZigBee operating in same environment using the same 2.4 GHz radio spectrum must attain the coexistence between themselves. To meet the quality-of-service (QoS) requirements [21] an IoT network major challenge is to achieve coexistence between different wireless technologies sharing 2.4 GHz ISM unlicensed spectrum [19]. Technologies utilizing the same frequency band target precise, non-invasive, appropriate, and cost-effective monitoring. The successful channel access probability should be as high as possible with the coexistence of an interfering network [22]. In this section the impact of the coexistence interference on Bluetooth and other peripheral technologies on same frequency band is discussed. Three main technologies are considered: IEEE Std. 802.15.4, IEEE Std. 802.11b and Bluetooth. BLE devices are supposed to function with low duty cycles, appropriately fast rates, and low transmission power. These features of BLE make devices very susceptible to interference from other wireless technologies operating in the same environment [23].

Due to crowded frequency spectrum, networks suffer a significant mutual interference and performance degradation. Coexistence between different wireless technologies can be categorized as space, time, and frequency domain. Coexistence can be achieved by fulfilling the dedicated requirements of the above-mentioned field. Adequate frequency separation between the networks, adequate spacing between the networks and controlled time-sharing of the channels helps to fulfil coexistence between technologies and QoS for rising wireless technologies. If the coexistence issue is not addressed properly then the network reliability and latency issues occur which leads to application failure. For example, WBANs are used in different areas with different devices and other devices with other wireless technologies exist and interfere. More the devices within a short distance, more will be the traffic densities, which may affect the operation of the technologies. To address the coexistence issues, one must consider the behaviour of the design, architecture, MAC, physical layer, and QoS [21], [22].

Considering the huge quantity of devices operating together, there are parameters which affect the performance of each individual device. These parameters are packet size, offered load, network topology, FH rate, spread spectrum, transmission power, error correction, traffic nature, and modulation scheme [20]. As these 2.4 GHz ISM band are world-wide and widely used the traffic density is dense so the impact of one system on the other is high. Different traffic shaping techniques and channel models has been considered to reduce the effect of interference for traffic data. The effect of the adjacent channel interference is on the bit-error rate, which must be considered when the coexistence problem is addressed [21].

All the medium access control aspects like frequency hopping, traffic load, packet structure along with transmission aspects like modulation format, propagation effect, interference, and thermal noise as well coding techniques are to be considered while solving coexistence issues [18]. Also, the transmission in LOS and NLOS conditions plays major role [24].

Due to the emergence of various wireless technologies in 2.4 GHz ISM band, the common RF spectrum is utilized in an un-coordinated that results in complexity and high uncertainty to medium. This affects the reliability and availability of wireless networks. Cross-technology interference (CTI) occurs due to simultaneous applications running in devices using unlicensed ISM band. These applications must inter-operate in a crowded frequency network so that coexistence is achieved. Although channel hopping and carrier sense multiple access/collision avoidance (CSMA/CA) methods improved communication reliability, CTI effect occurs when there are data transmissions in the same frequency spectrum by different standards. The effect of the CTI must be studied before we propose a solution to coexistence issue [21], [25].

3.1. Multiple access methods

The word "Coexistence mechanisms" is an integral part in developing any communication device. An operating wireless device will face interference if other wireless devices are operating at the same time. So, the interferer (another wireless device) frequency overlaps with the operating wireless device. To avoid the interference, the operating device can transmit information at different frequency than the interferer which is called frequency division multiple access (FDMA). The operating devices can transmit at different slots, called as time division multiple access (TDMA).

TDMA are convenient to low bit rate application environment where operating devices are using the same frequency space. TDMA technology is best suited to those applications which can wait until the channel is clear before sending the data. For example, for the streaming of wireless audio transmission applications, continuous use of the frequency is needed so FDMA is preferred over TDMA in this case. For wireless audio transmission a minimum of 2 Mbps audio capacity is needed [1], [26]. The audio data carried with this capacity have high radio duty cycle, so in this case TDMA is not the best solution to achieve coexistence.

FDMA techniques can be divided into FHSS, fixed channel assignment, and dynamic channel selection. FHSS, as used by traditional Bluetooth divides the ISM band spectrum into 79 channels spaced at 1 MHz [2]. The hopping is from channel to channel on a pre-determined schedule. So, if any packet is corrupted when transmitted on a given channel, it is immediately re-transmitted over another channel. AFH was also introduced to FHSS, which modifies FHSS hopping schedule based on the detected interference. This requires a minimum of 20 channels (20 MHz) in the hopping schedule.

FDMA dynamic channel selection allows the communicating device to be stayed on the selected channel by monitoring the effective throughput. So, it allows to switch channel if the interference persists. Dynamic channel selection also help to minimize the interference generated to allow other device operation to achieve the acceptable performance operating at the same ISM band [26].

In the fixed channel assignment approach, based on the environmental channel surroundings. Fixed channel assignment is used for fixed installation application such as WLAN which relies on TDMA techniques to deal with the interference.

Transmission power control allow a device to reduce the output power to the minimum required power for the acceptable performance. So, this technique helps to achieve the coexistence by minimizing the interference on the other devices sharing the ISM band [27].

Code division multiple access (CDMA) is another digital technique which takes digitized version of an analog signal and spreads it out over a wider bandwidth at low power level. This technique is also known as direct sequence spread spectrum (DSSS). The third generation (3G) cell-phone technology called wideband CDMA (WCDMA) uses spread spectrum method in a 5 MHz channel to allow multiple users to share the same band [26] .

3.2. Channel models

Different analytical and simulation model to compute the performance of Bluetooth under the interference of wireless technologies like ZigBee and Wi-Fi can be found and no exact experimental approaches can be drawn as the nature of the wireless channel and environment is complex. Due to the growing acceptance of wireless technologies, the frequency spectrum is congested. The accessible spectrum is limited and firmly controlled by the regulators [28]. In this work, ZigBee is the source of interference to the Bluetooth performance measurement. Paper [18], [19], [20], [21], [28], and [29] provides empirical studies on the coexistence between different wireless technologies under ISM band and in all cases, the interference of no more than two technology has been studied at a time.

Table 7 enlist the channel specification of the important technologies under ISM band. For each technology the occupied frequency band, channel bandwidth, modulation scheme, bit rate, and transmit power details are presented.

Table 7. Channel characteristics of BLE, Bluetooth, ZigBee, and Wi-Fi

Technology	Frequency band	Channel bandwidth	Modulation	Bit rate	Transmit power
BLE	2401 MHz-2481 MHz	2 MHz	GFSK	1 Mbps	-20 to 10 dBm
BLE 5	2401 MHz-248 1MHz	2MHz	GFSK	1Mbps(LE1M) 2Mbps(LE2M) 500 kbps or 125 kbps(LE coded)	-20 to 20 dBm
Classical Bluetooth	2401.5 MHz-2480.5MHz	1 MHz	GFSK π/4DQPK 8DPSK	721 kbps 3 Mbps 24 Mbps	0 dBm 4 dBm 20 dBm
IEEE Std. 802.15.4	868 MHz 915 MHz 2.4 GHz UWB: 249.6 to 749 MHz 3.1 to 4.8 GHz 5.8 to 10.6 GHz	868 MHz 915 MHz 2.4 GHz UWB: 500 to 1354 MHz	BPSK O-QPSK UWB: BPM -BPSK	20 kbps 40 kbps 250 kbps UWB: 0.11 to 27 Mbps	-32 to 0 dBm
IEEE Std. 802.11 b/g	2.4 GHz	22 MHz	DSSS/ OFDM	1-54 Mbps	20 dBm

In this section the channel allocation in frequency spectrum of the three technologies namely 802.15.1, Wi-Fi and Bluetooth are presented. The channel allocation and potential overlap with other technologies are presented in Figure 12.

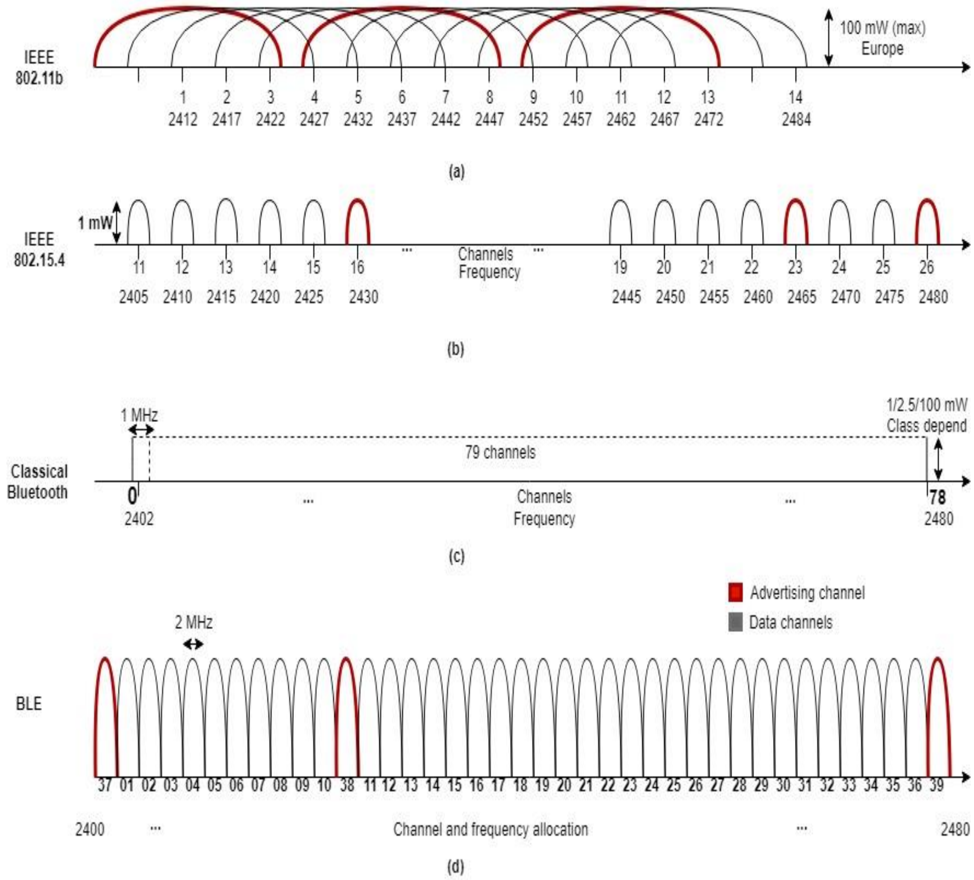

Figure 12. Channel overview.

3.2.1. IEEE Std. 802.11b / Wireless fidelity (Wi-Fi)

IEEE Std. 802.11 defines the WLAN MAC layer and PHY specifications. The Wi-Fi specify that compliant device operate with each channel bandwidth of 22 MHz with channel separation of 5MHz in the ISM band. In the 2.4 GHz band, the IEEE Std. 802.11b/g supports up to 14 channels [28]. 13 channels are specified for the Europe and 11 channels for America and channel 14 is allowed only in Japan for IEEE Std. 802.11b. To support the data rates, different air interfaces and modulation schemes are developed. For example, orthogonal frequency division multiplexing (OFDM) is used to provide up to 54 Mbps data rates for IEEE Std. 802.11b and complementary code keying (CCK) is used to provide up to 11 Mbps data rates for 802.11g and 72Mbps for IEEE Std. 802.11n using a single stream on a single channel.

From the Figure 12(a), we can notice that the spectral width (22 MHz) of IEEE Std. 802.11 channel is four time than IEEE Std. 802.15.4. One approach to achieve the maximum throughput by non-overlapping channels is to utilize the common pattern for using IEEE Std. 802.11 channels in such way that channel 1,6 and 11 are in usage. For the 5GHz band, transmit power control (TPC) and dynamic channel selection routes have been defined for the device operation to make the operation more adaptive and optimize the available resources. In the 2.4 GHz band, the maximum transmission power is 1 W (30 dBm) in America, 100 mW (20 dBm) in Europe and, 10 mW/MHz in Japan.

3.2.2. IEEE Std. 802.15.4

The IEEE Std. 802.15.4 is developed for low-rate wireless PAN, which specify a total of 27 channels among which 16 channels are in the 2.4 GHz band, 10 channels in the 915 MHz band and 1 channel in the 868 MHz band targeting short range communication as shown in Figure 12(b). Typically, the targeted distance is up to 10 meters with maximum theoretical data rate for the above-mentioned bands are 250 kbps, 40 kbps and 20 kbps respectively. The 2 MHz channel is much narrower as compared to Wi-Fi channel. The transmitting power is up to 1mW and offset-quadrature phase shift keying (O-QPSK) [28] modulation scheme is utilized. All the 16 mentioned channels do not overlap so the coexistence with other ZigBee devices is achieved easily and networking in the same area is easily achieved. IEEE Std. 802.15.4(ZigBee) based wireless sensor networks (WSN) are vulnerable to interference as compared to Bluetooth and Wi-Fi network. The channel hopping is not supported by IEEE Std. 802.15.4 as compared to Bluetooth; therefore, a selected channel is not changed.

In the 2.4 GHz band, DSSS modulation and CSMA/CA or TDMA allowed for access to channel with multiple participants. CCMA/CA monitors the channels with different three modes. CCA Mode 1 [28], [30] represents the energy above threshold condition and if radio detected energy level above threshold, busy medium is acknowledged. CCA Mode 2 used as carrier sense. When the radio identifies a signal, which is modulated and spread, it acknowledges the medium as busy. The third mode CCA Mode 3 acknowledges the medium as busy when the carrier sense signal energy above a defined threshold. When the medium is busy, transmission time is longer so as the latency increases.

The channel allocation of ZigBee and Wi-Fi channels under ISM band is as shown in Figure 13.

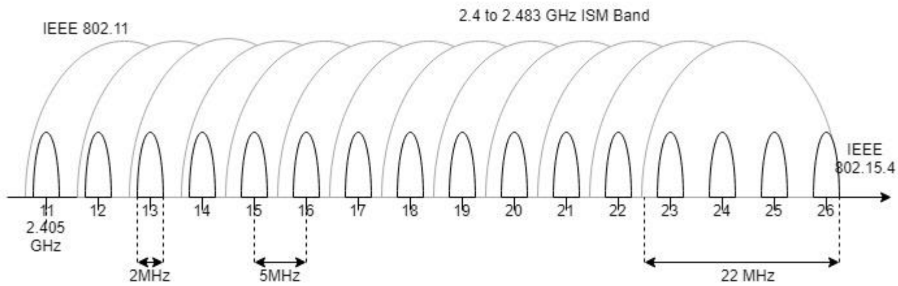

Figure 13. Channel occupancy of IEEE Std. 802.11 and IEEE Std. 802.15.4.

Each Wi-Fi channel is 22 MHz wide and ZigBee channel is 2 MHz wide. Note that, one Wi-Fi channel completely overlaps four ZigBee channels. In Wi-Fi channel allocation, the three most non-overlapping channels are 1, 6 and 11. So, the ZigBee channels 14 and 15 (the rightmost) should be free from interference from Wi-Fi transmission. One of the difficulties to achieve the coexistence between Wi-Fi and ZigBee is due to different allowed transmission power. The maximum ZigBee transmission power is 1mW which is very low as compared to the maximum Wi-Fi transmission power of 100 mW. Since two ZigBee channels are assumed to be free of interference from Wi-Fi, two channels might not be enough to allow coexistence among several geographically overlapping PANs [30].

IEEE Std. 802.15.4 has two different operational mode: beacon-enabled and non-beacon-enabled mode. The non-beacon-enabled mode is not time structured and hence does not implement duty cycling [29]. The beacon-enabled mode divides transmission time to beacons intervals (BIs) as super frame duration (SD) and Inactive or sleep period as shown in Figure 14.

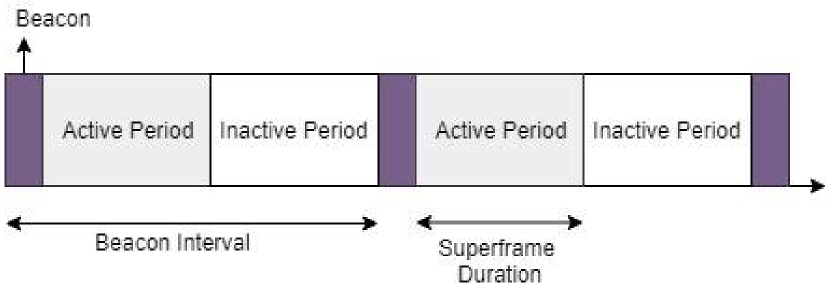

Figure 14. Time-domain structure of beacon-enabled IEEE Std. 802.15.4.

3.2.3. IEEE Std. 802.15.1 /Bluetooth

Bluetooth communication protocol (IEEE Std. 802.15.1) uses 79 radio frequency channels in the 2.4 GHz band. Each channel is 1MHz wide as shown in Figure 12(c). In order to avoid interference, Bluetooth technology utilizes the FHSS, to spread the signal across the dedicated 79 channels with a forward error correction (FEC) coding technique [24]. Bluetooth use packet-based structure in a master-slave arrangement and utilizes the full available 2.4 GHz band. The switching of the carrier channel is rapid at the rate of 1600 hops per second. In the 79 determined pattern of channels, six different types of hopping sequences are defined. Each 1 MHz channel are adjacent to its former and inheritor channel. Due to FHSS, the Bluetooth technology can have different hopping patterns or a time-shifted patters result in more resistive to the interferer and can coexist in the same area where number of different networks are available.

AFH scheme helps Bluetooth to avoid channels that are busy and are used by other technologies such as IEEE Std. 802.11. Bluetooth channel quality determines the data rates to be provides in order to adapt to the communication environmental with adaptive power control feature. In Bluetooth three different classes have been defined based on the sending power as 1, 2.5 and 100 mW [28], and accordingly a reference range have been specified as 1, 10 and 100 meters respectively.

3.2.4. BLE and Bluetooth 5

BLE can provide connectivity with less power as compared to classical Bluetooth. The BLE 5 signifies additional development of the BLE technology, which broadly addresses the key problems of its precursor, namely the long transmission times, limited functionality, and limited range of the broadcasting ways. The problem of improving the communication range and the maximum throughput has been addressed in BLE 5 specification. Three new PHY alternatives has been hosted in BLE 5. In addition to 1 Mbit/sec GFSK [9] of BLE 4 (namely addresses as LE 1M), the BLE 5 signifies a 2 Mbit/sec GFSK PHY (LE 2M) for short-range high-speed transmission and two coded PHY with payload coded at 500 kbit/sec or 125 kbit/sec as shown in Table 7.

BLE utilizes the adaptive AFH technique which automatically blacklist the low-quality channels during the transmission where channel changes after every CE. In this way the BLE and BLE 5 are more resistive to the interfering networks [29].

The channel access model in Bluetooth is based on the master-slave configuration, which is built on the time division duplex (TDD) transmission scheme. BLE sends data in two different ways: namely connection-oriented periodic data trade and connectionless broadcasting. In connectionless broadcasting there is no use of duty cycle and it is not time structured. In connection-oriented transmission, at least one slave is connected to the central node (master). The transmission time is divided into periodic connection intervals (CIs) and each CI includes a CE, which is the data transmission period and a sleeping time [29]. The time-domain structure of Bluetooth in connection-oriented transmission is shown in Figure 15.

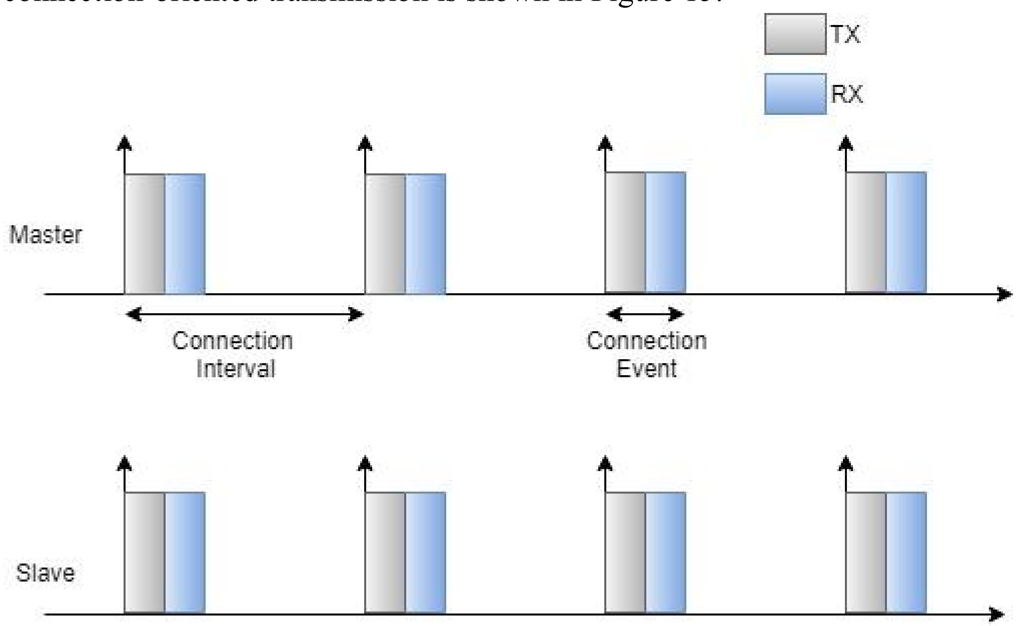

Figure 15. Time-domain communication in Bluetooth.

3.3. Coexistence and discussions

From the above-mentioned channel overview in Figure 12, and performance explanation of different technologies, it is clear that a large variety of wireless technologies are using the most crowded unlicensed 2.4 GHz bands. In realistic network scenarios, it is found that BLE is affected more by IEEE Std. 802.15.4 interference than vice versa [30]. Since IEEE Std. 802.15.4 have longer channel-occupancy as compared to BLE, BLE is more resilient than IEEE Std. 802.15.4 against IEEE Std. 802.11 interference. The coexistence issue in the 2.4 GHz ISM band is still a topic to research and to develop techniques to mitigate the problem, because more new wireless technologies are either emerging or in the development process.

Based on paper [30], the experimental result analysis to test the impact of three different technologies in unlicensed band transmission is presented below. The Wi-Fi transmission is barely affected by the presence of Bluetooth and ZigBee interference in the parallel as well as crossed configuration. When the experiment was taken to the worst condition i.e. the interference nodes near to the Wi-Fi receiver, Wi-Fi did not show any noticeable loss. Both Bluetooth and ZigBee transmission suffer performance degradation in the presence of the Wi-Fi interference. Data shows ZigBee performance drop was 41% on average while Bluetooth degradation was more (68%) as compared to ZigBee in the presence of Wi-Fi interference. In the measurement scenario of Bluetooth transmission under the ZigBee interference where both the devices are operating in the same physical space it was found that the Bluetooth is highly influenced by the ZigBee interference than vice versa. To mitigate this interference proper control of the power levels and duty cycle of the Std. 802.15.4 devices, as well BLE frequency hopping is useful.

Paper [24] presents an analytical method to evaluate the performance of Bluetooth transmission interfered by the Wi-Fi and vice versa in a fading channel with additive white Gaussian noise (AWGN). The performance of the two technologies were evaluated in terms of the packet error probability (PEP) considering all the parameters presence as thermal noise, interference, coding techniques, propagation impairments, and modulation scheme together with frequency hopping, traffic load and packet structures. The presence or the absence of LOS propagation as well as system parameters i.e., effect of the coexistence distance, transmission power. The result shows that two system can simultaneously operate in the same environment only if the desired QoS, is guaranteed for the both. The interference effect is strongly dependent on the transmitted power level and to reduce the interference effect a properly designed adaptive utilization of transmitted power could be useful.

Paper [31], which is based on experimental measurement at hospital highlights the diverse medical wireless application as well other wireless system to work normally without the need of control to performance parameters even at the peak hospital hours. For medical scenarios, paper [32] develop a wiser concept. They propose a generic protocol stack model that recognizes the presence of the heterogeneous networks. Basically, this stack model uses common features of the wireless devices and implements a cognitive procedure for the layers to share available information to each corresponding protocol stack.

Paper [29] presents the time domain cooperative coexistence of the Bluetooth and IEEE Std. 802.15.4 network. They develop a cooperative mechanism to avoid overlap of communications in the mentioned communications so that the CTI is decreased that results in proper time synchronization between two technologies. The idea is to set the active transmission period of one technology in such way that, it is not the multiple of other one i.e., simultaneous transmission takes place. The proposed algorithm predicts the packet collision time and avoid them by shifting the periodic transmission. The experimental result showed 12 % improvement in packet delivery with this approach.

4. MEASUREMENT DEVICES

In this work, two nRF52840 [8] chipset was used, which is the first commercial chipset from the Nordic Semiconductor that supports BLE 5.0. This chipset was programmed with S140 SoftDevice v6.0.0 [8]. The SoftDevice is precompiled and linked binary software implementing Bluetooth protocol developed by Nordic Semiconductor. Three ZigBee nodes CWC-MOD-POW (version two) were used as the interference.

4.1. nRF52840 Development kit (Dk) and S140 SoftDevice

The nRF52840 [6], [8] is fully multiprotocol radio capable with protocol support for Bluetooth 5. In this work, two nRF52840 preview DK were used. The hardware in Figure 16 and Figure 17 shows the front view and back view of the board.

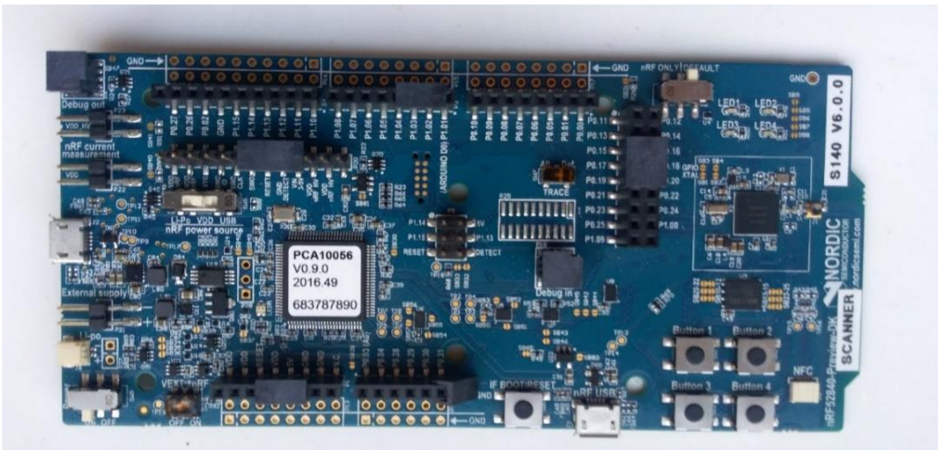

Figure 16. nRF52840 front-view.

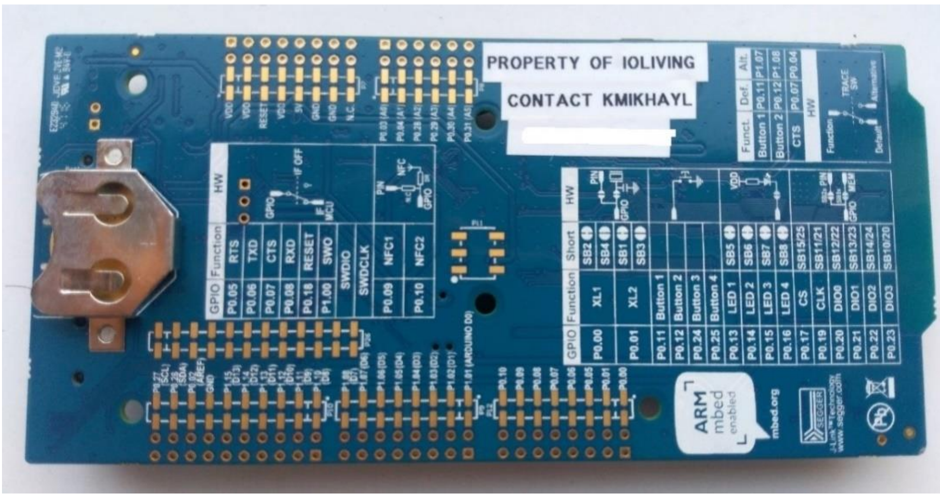

Figure 17. nRF52840 back-view.

The nRF52840 system on chip (SoC) meets the prerequisites for the BLE 5 by offering generous memory for both random access memory (RAM) and flash. nRF52840 multi-standard chipset is developed around 32-bit ARM Cortex-M4F based microcontroller with 64 MHz oscillator. The chipset is built to support different data rates from 125 kbs to 2Mbps based on the requirements. For Bluetooth 5, the supported data rates are 2 Mbps, 1Mbps, 500kbps and 125kbps. The sensitivity for 1Mbps and 125 kbps BLE are -95 dBm and -103 dBm respectively [33].

Further, this sophisticated chipset nRF52840 supports on-chip adaptive power management for all peripherals along with on air compatibility with other nRF series. This chipset provides programmable output power from +8dBm to -20dBm, ARM Trust Zone crypto Cell cryptographic unit supports extensive cryptographic options [8]. The application field approached by nRF52840 can be categorized into three main field as advanced wearables, interactive devices and IoT. In advanced wearables many products related to connected watches, VR, connected health, wearables with wireless payments, personal fitness has been developed. Advanced remote controllers as well gaming controllers are some application under interactive devices. IoT is a broad field which can be a home automation concept as well industrial IoT sensors and controllers, and many other applications [33].

The DK board PCA10056 is used as a development platform for the nRF52840 SoC which provides on-board debugging as well as programming solution. This chipset was programmed with S140 Soft Device v6.0.0, which is precompiled and linked binary software implementing BLE protocol developed by Nordic Semiconductor. One of the boards was used as an advertiser and another as scanner. In the board controls buttons were available to choose BLE PHY as LE 1M, LE 2M or LE coded [8]. For example, mode 1 Buttons supports LE 1M and mode 3 buttons as LE coded. The firmware for the two DK was based on ATT_MTU Throughput Example of the nRF5 SDK v15.0.0.

The nRF52840 DK has a 64 Mb external flash memory which is multi I/O memory that supports both regular serial peripheral interface (SPI) and quadrature serial peripheral interface (QSPI). The four buttons and four light emitting diodes (LEDs) are connected to dedicate general purpose input/ output (GPIOs) on the development board. The nRF52840 DK offers range of applications such as Bluetooth 5, BLE, Thread, ANT, IEEE Std. 802.15.4, ZigBee and 2.4GHz proprietary using multi-protocol nRF52840 SoC. This kit contains an integrated printed circuit boards (PCB) and RF connector as well for the direct RF test measurements. All the 48 I/O pins and interfaces are accessible in the kit via connectors.

The main features of the DK are highlighted as [33]

- Supports NFC-A listen mode
- Bluetooth 5 multi-protocol radio with 2 Mbps speed, long range, improved coexistence and advertising extensions
- 4 user programmable buttons, 4 user programmable LEDs
- +1.7v to +5.5v operation from USB, external source or battery
- All I/O pins and interfaces available via connectors
- I/O interface for Arduino form factor plug-in modules
- Compatible with Nordic power profile kit
- nRF52840 flash-based ANT, ANT+, BLE, Bluetooth5 SoC solution
- Flash memory
- Drag-and-drop mass storage device (MSD) programming
- UART interface through virtual communication (COM) port

The nRF52840 SDK offers developers a variety of modules for building fully featured, secure and reliable applications with the DK. The SDK provides a rich developing platform for nRF52840 device by including a broad selection of libraries, SoftDevices, drivers, examples for peripherals, and proprietary radio channels.The chipset nRF52840 is programmed with S140 SoftDevice v6.0.0, which is the central as well as peripheral protocol stack solution for the BLE and Bluetooth 5. For the implementation of Bluetooth 5, S140 works as a preoccupied and coupled binary software advanced by Nordic Semiconductor. This SoftDevice supports all the features of Bluetooth 5 [2].

The SoftDevice consists up of three main components as SoC library, SoftDevice manager (SDM) and Bluetooth 5 LE protocol stack and application programming interface (API). The SoC library manages the application coexistence for shared hardware resource management. SDM function for enabling or disabling the SoftDevice state and configures the behaviour of SoftDevice core functionality. The API is a set of C functions that give the application complete compiler and linker from the SoftDevice implementation. All SoftDevice API function performance status is checked using a 32-bit error code.

4.2. Received signal strength indicator (RSSI) and packet layout

Radio Device Address match unit and interface spacing unit are the additional features to support Bluetooth smart and similar IoT applications. The radio also defines bit counter and RSSI. Bit counter counts the received or sent bit by the radio and generated event based on configured number [8]. The radio sends different sub packets in order from left to right as shown in Figure 18.

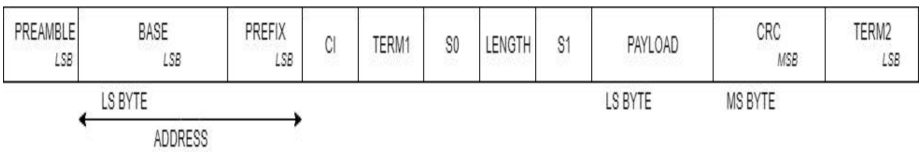

Figure 18. On-air packet layout.

A radio packet contains PREAMBLE, ADDRESS, SO, LENGTH, S1, PAYLOAD and CRC. The PREAMBLE is defined based on mode used. For example, for mode 250kbit PREAMBLE is 4 bytes long and all set to zeros and for 2Mbit PREAMBLE is 2 byte long. The ordering byte is Least Significant Byte (LSB) first for ADDRESS and PAYLOAD field and Most Significant Byte (MSB) first for CRC field. S0, S1 and LENGTH are specified with length and accordingly memory allocation is done. In case, if these field are specified zero length then their field will be omitted in memory. The maximum defined length for S0, S1 and LENGTH together is 258 bytes.

The on-air ADDRESS field contains two part, the base address and prefix address with respective registers for them. The CRC calculates the redundancy over the whole packet excluding the preamble. The CRC is calculated by feeding the packer serially through CRC generator. The RSSI indicates the power in the received radio signal. The sampling of received signal is started by RSSISTSRT task which read samples from RSSI sample register.

4.3. Advertiser

BLE uses 40 different frequency channels (PHY channels) and the spacing of each channel is 2 MHz. Among 40 channels, 3 channels are known as Primary Advertisements channels and the remaining 37 channels are known as Data channels or Secondary Advertisements channels as shown in Table 8. Advertisements are used by Bluetooth device to broadcast information and data for another scanner device to discover and communicate. Advertiser operation follows the defined parameters and configurations. The experimental parameters and configurations for Advertiser are presented in Table 8, based on the different measurement modes. Note that Advertiser operation flow algorithm is presented in appendix part.

Table 8. Experimental parameters and configurations for Advertiser

Parameter	Mode 1	Mode 3
TX Power (dBm)	0	
Primary advertisements channels IDs	39	
Secondary advertisements channels IDs	0,1,2,3,4…….,36	
Advertisement payload (Bytes)	12	
Primary advertisement channel PHY	1 Mbps	CODED (S=8)
Secondary advertisement channel PHY	Not Set	CODED (S=8)
Advertising delay (ms)	50	
Serial interface period(seconds)	1	
Serial interface configurations	End of line: CR+LF, no parity, UART, 115200 bps data rate, 1 stop bit, 8 data bits	

The three Primary Advertisement channels initializes the advertisement process as primarily the advertisement packets are sent to these three channels. Channels 37, 38, and 39 are allocated as Primary Advertisements and are divided into advertising events where each event can occur on each of 3 advertising PHY channels or a subset. Consecutive events start with the first advertising PHY channel and events occur at regular interval. Scan request or the connection request is possible on the same advertising PHY channel.

Channels from 0 to 36 are named as Secondary Advertisement channels or Data channels. Data channels are not the part of advertisement event but play vital role as extended advertisement event. The Secondary Advertisement begins at the same time as Primary Advertisement channel and end with the last packet on secondary channel. Data channels can make any PHY selection (LE 1M PHY, LE 2M PHY or LE Coded) but the advertising packets in the secondary channel should use same PHY.

Advertisement can be categorized into two groups as: Legacy Advertisement and Extended Advertisement. Legacy Advertisement were introduced in BLE 4.0, 4.1, 4.2, and exist in 5.0. Extended Advertisement are introduced in Bluetooth 5.

4.4. Scanner

Scanner operation follows the defined parameters and configurations. The experimental parameters and configurations for scanner are presented in Table 9, based on the different measurement modes.

Table 9. Experimental parameters and configurations for Scanner

Parameter	Mode 1 BLE	Mode 3 Bluetooth 5
Primary advertising channels IDs	39	
Secondary advertising channels IDs	0,1,2,3,4………..,36	
PHY	1Mbps	CODED (S=8)
Operation mode	Non-extended	Extended
Serial interface report period (seconds)	1	
Serial interface configurations	End of line: CR+LF, no parity, UART, 115200 bps data rate, 1 stop bit, 8 data bits	

The BLE scanner captures advertisements based on defined advertising characterises and PHY mode: 2Mbps, 1Mbps, or PHY coded. In this work, the beacon scanner processes the captured advertisements through serial port. The application simply reads beacon advertisements and prints it by serial port.

4.5. ZigBee

Three pieces of CWC-MOD-POW platform version two [34], [35] as shown in Figure 19 was used in order to introduce interference while measuring the performance of Bluetooth 5.

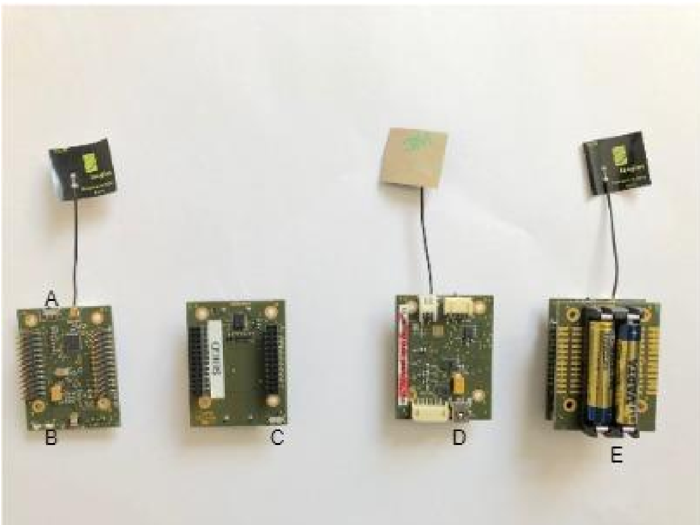

Figure 19. Photos of ZigBee modules and assembled node (A- reset switch, B- Indicator LEDs, C- Power switch, D- mini-USB power connector, E-AAA battery holders).

The main board of device is built with Texas Instruments CC2650 [36] ULP wireless micro controller unit (MCU) platform which can be used for wide range of applications. The core middleware is based on TI CCS 7.4.0.00015 IDE and CWC CC2650 IEEE Std. 802.15.4 proprietary driver and firmware. The receiver sensitivity for 802.15.4 is -100dBm respectively. The CC2650 based device is 32-bit ARM Cortex-M3 processor which operate at 48 MHz as main processor to enable short processing times and high integration. The ZigBee firmware configuration and specification are presented in Table 10.

Table 10. Firmware configuration and parameters

Label	Specification
payload per frame	116 bytes
frequency channel	26
operating frequency	2480
Transmission power	0 dBm

Some of the advantages of using Cortex-M3 processor are high-performance, low cost which fulfils optimized embedded applications [37]. Some of the CC2650 based low-power wireless application are electronic labelling, WSN, consumer electronics, remote controls, smart metering, home and building automation, lighting control, alarm and security, medical, sports and fitness application, mobile phone accessories and asset tracking. Some of the features of Cortex-M3 [36] processor are fast code execution to increases sleep mode time, ULP consumption, Harvard architecture-based buses for instruction and data, efficient processor and memories, high-performance interrupt handling for time-critical applications, efficient processing performance with fast interrupt handling.

4.6. Taoglas

The ZigBee nodes are equipped with an external antenna, Taoglas FX70.07.0053A [38], which can be seen from Figure 19. The FX70 is multi standard freedom 2.4 GHz supporting low profile and high-performance magnetic field antenna. Installation of antenna is easy through cable connection. Different communication system like Bluetooth, Wi-Fi, and ZigBee in 2.4 GHz ISM supports Taoglas. Some of the features of TaoglasFX70 are 80% antenna efficiency, 5 dBi gain, linear polarisation, -20 dB return loss, 5 watt power handling, 1.5 dBi free space peak gain, sufficient operation temperature (-40 °C to +85 °C), less dimension (27*25*0.08 mm) and Restriction of Hazardous Substances (RoHS) compliant [38].

5. EXPERIMENTAL PERFORMANCE EVALUATION

In this work, two pieces of the nRF52840-Preview- DK (PCA10056) and three ZigBee nodes CWC-MOD-POW were used for the Bluetooth 5 performance evaluation as shown in Figure 20. One laptop is used with installed HTerm terminal program [39] for the recording of the scanned data. USB cable was used for connecting scanner to the laptop. One of the boards was designed as an advertiser, and the other one as scanner. 4 different controls buttons are embedded in the DK, so the required BLE PHY option can be chosen (i.e., LE 1M, LE 2M, or LE Coded).

Figure 20. Devices used for measurement.

The flowchart of measurement procedure is shown in Figure 21. Once the BLE boards are positioned in the specified locations, the laptop was connected to the scanner (receiver) via a USB cable, configured to proceed using the required PHY layer choice. On the Laptop, the HTerm terminal was running during the entire measurement. On the other side advertiser was powered with battery. The advertiser was continuously transmitting packets. On android phone, Wi-Fi analyser was running in between measurement to check if the allocated channels overlap. Sniffers were used to find out interference other than ZigBee, such as from Bluetooth or Wi-Fi signal spectrum while taking measurement. There was no other interference from other Bluetooth or Wi-Fi signal.

The scanner was enforced to regularly scan every single advertisement channel, and every second the scanner recorded the number of the received advertisements from the advertiser board via serial interface, as well as the RSSI and the sequence identifier for the last advertisement it has received. Each single advertisement was assigned with a unique sequence number by the advertiser and the transmission of advertisement is periodic.

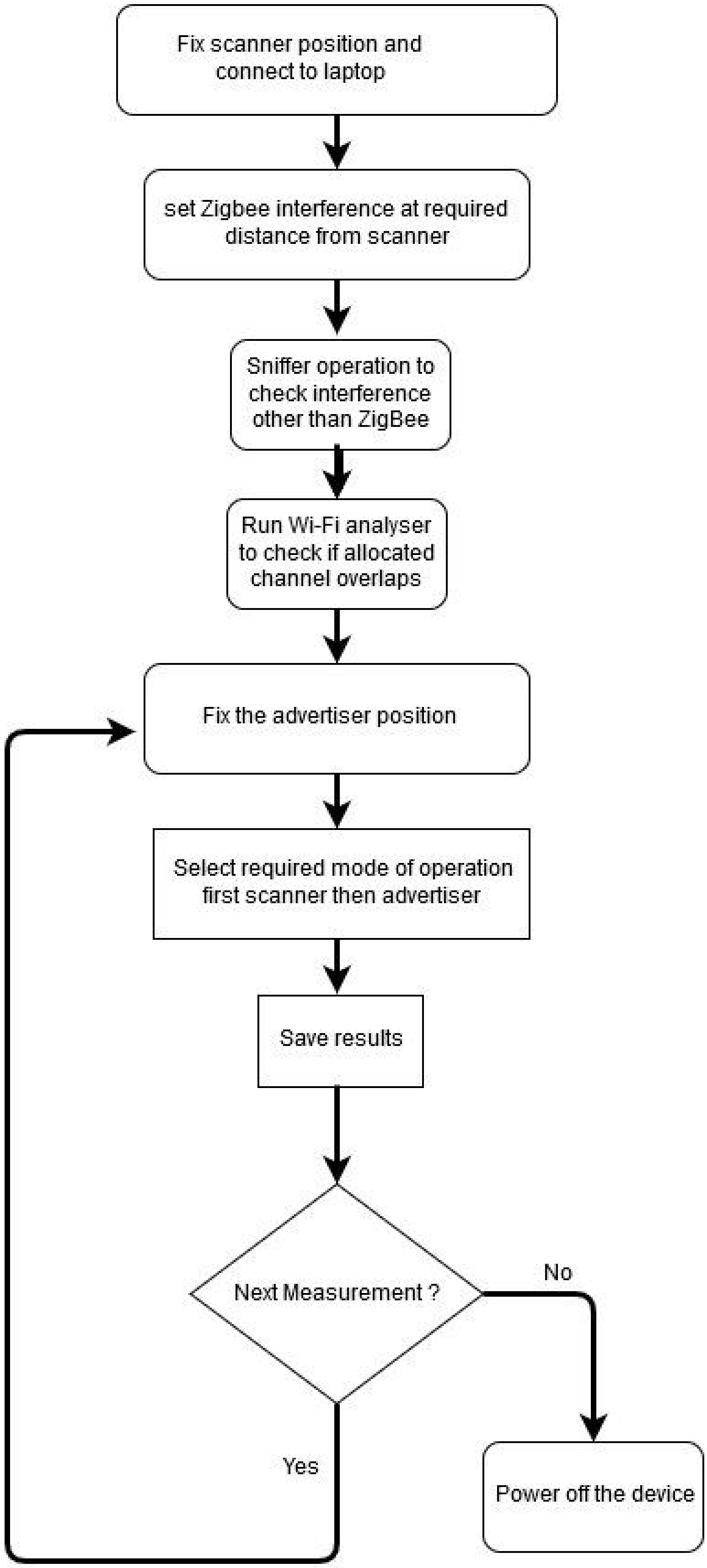

Figure 21. Flowchart of measurement procedure.

The designed figurative approach to take measurement is shown in Figure 22, where TX and RX represents two nRF52840 as the advertiser and scanner respectively. Node 1, 2 and 3 are the three pieces of ZigBee nodes placed in a circle form so that the three interferers were at the same distance from the scanner. Distance between the advertiser and the scanner is represented by “d”, which in our experiment varies between 4 m to 14 m in LOS measurement.

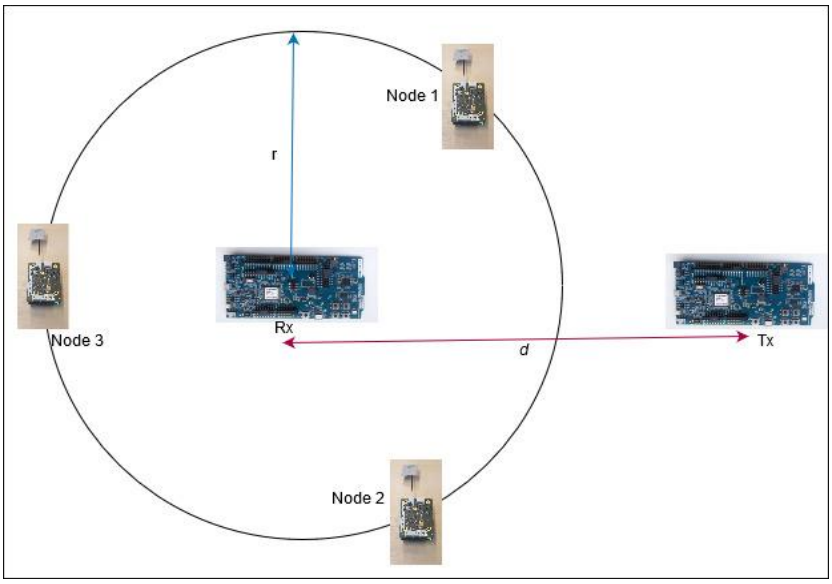

Figure 22. Measurement scenario, metaphorical representation.

Measurements were taken at a restaurant (Napa) premise at the University of Oulu during the vacation period. The restaurant was not open for customers that could interfere measurements. The abstract field arrangement of the devices is presented in Figure 23.

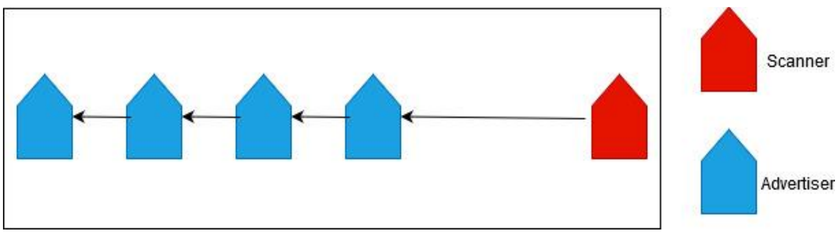

Figure 23. An abstract sketch of the experimental LOS scenario.

The blue device structure represents the transmitter which sends one same packet periodically. Another red device structure represents the receiver which receives packets and calculates throughput. The distance between two devices was gradually increased by moving the transmitter. Specifically, receiving of packets between 4 m to 14 m link distance. The BLE boards were set at the same height of 1 m so that the both antennae embedded on the device were at the same level and they were able to point each other creating LOS link. The interfering ZigBee nodes were placed around the BLE scanner, all at the same distance (case 1 = 4 m, case 2 = 6 m and case 3 = 10 m) to the BLE scanner.

The actual measurement scenario is presented in Figure 24. Different BLE link lengths were used and number of received advertisements were recorded for 10 minutes duration at each case so that on average 10 000 BLE packets being sent. At the end of the experiment, the PER was calculated from the total number of the packets receives by the scanner and the sequence number of the last received signal.

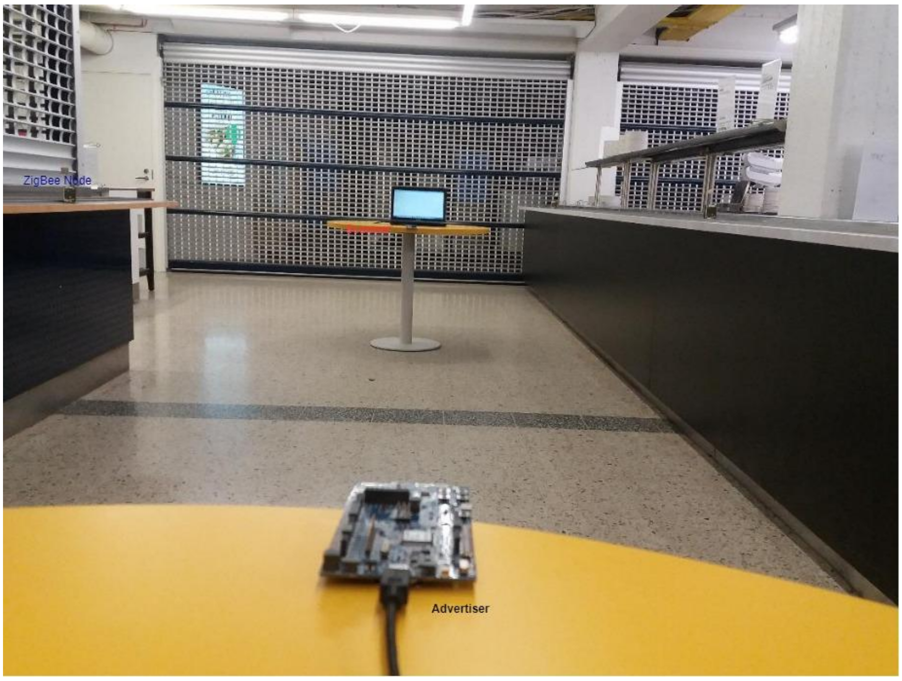

Figure 24. Actual measurement scenario.

Figure 25 shows recorded number of received advertisements by scanner. Sequence identification of the transmitted bit is represented by SEQ and NUMRX represents sequence identification of the received bit. RSSI information is also mentioned.

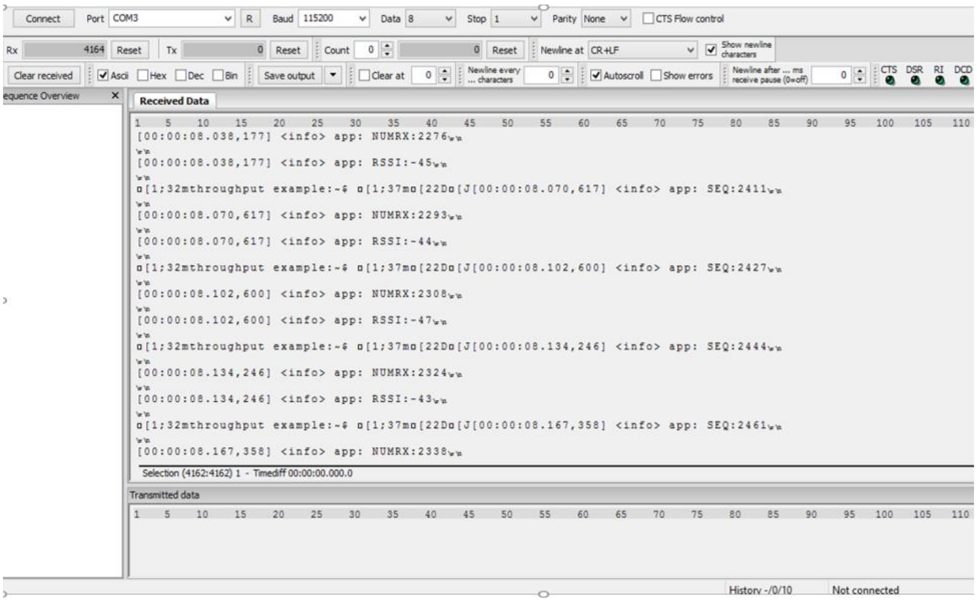

Figure 25. *Illustration of p*eriodic serial reports by scanner.

PER is number of erroneous packets divided by the total number of transmitted packets. PER is here defined to be *E,* and is calculated as

$$E = \frac{nTX - nRX}{nTX}, \tag{1}$$

where
E = packet error rate
nTX = number of transmitted packets
nRX = total number of received packets.

5.1. Results

In this section, the performance of the BLE under ZigBee interference is presented. During the whole process of experiment the transmission power set is 0 dBm. High data rates and longer range are not possible at the same time, two different modes of Bluetooth, BLE 4 and BLE 5 are considered under ZigBee interference. This thesis work was the continuation on analytical performance evaluation [6]. The analytical PER evaluation was done for BLE 5. After taking experimental measurement for BLE 4 and BLE 5, measurement results verified the analytical model results.

To evaluate BLE PER under ZigBee interference, the experimental scenario as explained above was implemented. Some of the important parameters used in experimental performance evaluation of BLE is listed in Table 11. Note that devices were using the same channel all the time. In addition, same parameters were set for the BLE 5 coded (s = 8) mode to find out gain achieved using FEC.

Table 11. Parameter settings for experimental performance evaluation

Parameter	**Value**
Frequency	2.4 GHz
BLE communication channel	CH #39
ZigBee communication channel	CH #26
Number of interfering nodes	3
Distance to interference	Case 1 = 4 m, Case 2 = 6 m, Case 3 = 10 m
Target Bluetooth length	4-11 m (case1 and case 2), 4-14m (case3)
Data Rate (BLE)	1 Mbps
Data Rate (ZigBee)	250 kbps
Transmit Power (BLE)	0 dBm
Transmit Power (ZigBee)	0 dBm
RSSI at 1m, BLE	-15 dBm

Figure 26 shows the performance of BLE 4 and BLE 5 under three ZigBee nodes interference. Here, x-axis represents the variable LOS BLE link length and y-axis represents PER. ZigBee nodes were set at 4-meter distance from the BLE receiver in order to create LOS interference. From Figure 26, it can be depicted that the effect of interference is transparent when the BLE 4 link distance is less than 5 meters. The increase in PER is rapid as the BLE link is increased and reaches its maximum value when BLE link length is 10 meters. After 10 meters the receiver was not able receive any packet. At the time of measurement, BLE 4 performance without interference was done, and it was found that till 80 meters link distance, the PER of BLE 4 link remained below 15%. BLE 5 coded mode seems to be more resistive to interference as compared to BLE 4 as error correction was applied. Until 8 meters, there is no packet loss. 3 meters higher communication range can be achieved with BLE 5 as compared to BLE 4 without packet loss. After 9 meters, the increment in PER is so rapid that the error correction is unable to mitigate against the interference created by the ZigBee nodes. In this experiment, the Bluetooth seems to be heavily affected by the ZigBee interference.

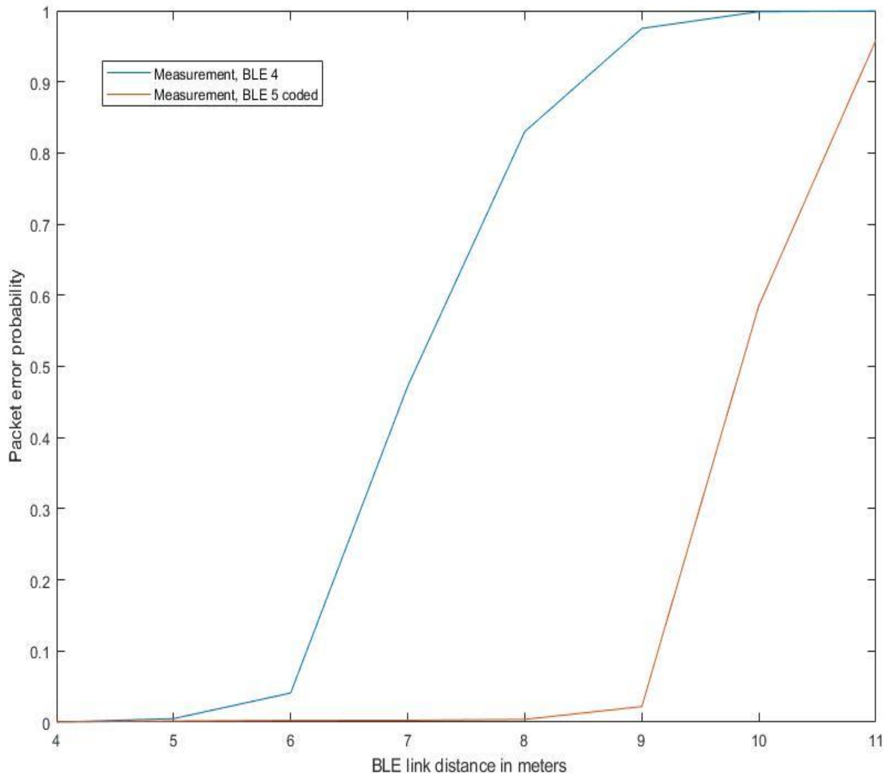

Figure 26. BLE PER under interference of three ZigBee nodes at 4m distance.

Figure 27 shows results for BLE performance as above, the setup is otherwise similar, but the interferers distance was increased to 6 meters. Due to longer interference distance, performance of BLE device seems better and results longer BLE link distance. In case of BLE 4, PER starts to increase rapidly as the BLE link length is increased beyond 6 meters and in case of BLE 5, after 9 m link length PER increases rapidly.

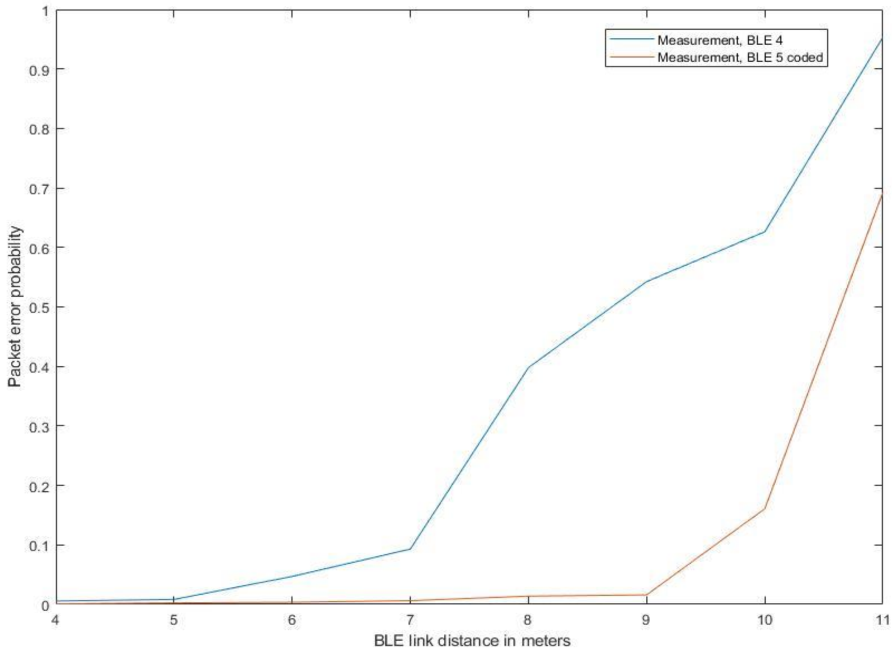

Figure 27. BLE PER under interference of three ZigBee nodes at 6m distance.

Further, Figure 28 shows the PER for the case where ZigBee nodes were set at 10 m distance from the BLE receiver and longer BLE link is observed. As the interference distance increased a bit more variation in the BLE link is observed. BLE 5 coded mode measurement results shows the coding gain of 2 to 3 meters in terms of increased BLE link length.

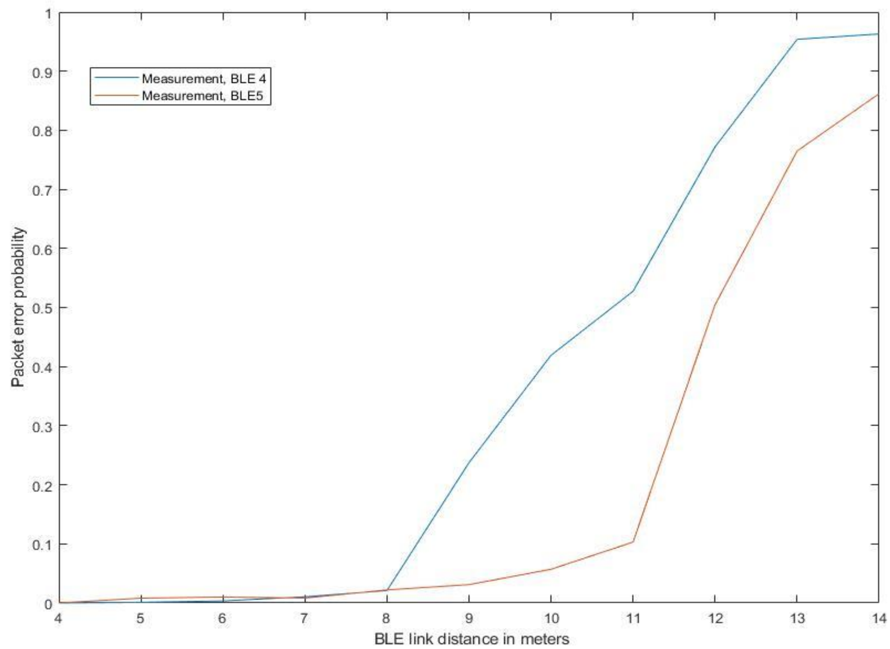

Figure 28. BLE PER under interference of three ZigBee nodes at 10m distance.

Figure 29 and Figure 30 shows the BLE achievable link distance under three different interference scenario of ZigBee with the PER target requirement less than 10%. Three circles represent different interference scenarios, the innermost circle area is the coverage of BLE when the interfering node is at 4 m, middle circle shows the coverage of BLE when the interfering node at 6m, and outermost circle represents the coverage of BLE when the interfering node is at 10 m. BLE 4 achievable range when the interference nodes are at 4 m, 6 m, and 10 m are 6 m, 7 m, and 8.2 m respectively with PER less than 10%. Further, BLE 5 achievable range for the same interfering scenarios are 9, 10, and 11 m respectively. From this data, it clearly shows that coding gain of one-third BLE link distance is achieved.

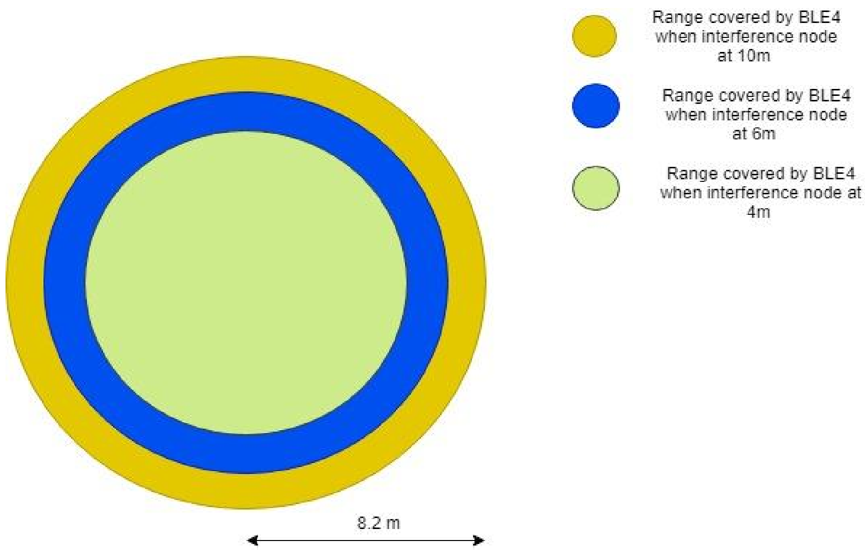

Figure 29. BLE 4 achievable range with PER<0.1.

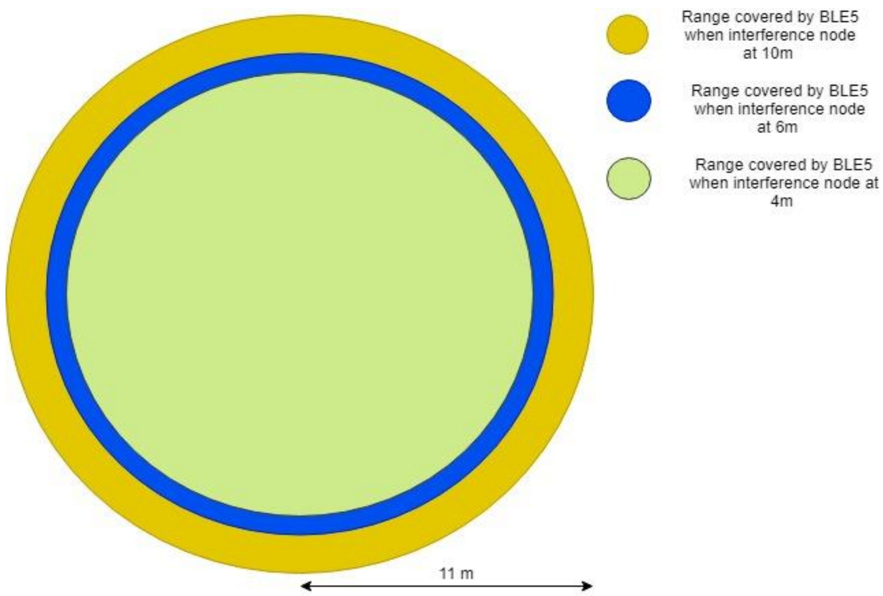

Figure 30. BLE 5 achievable range with PER <0.1.

RSSI indicates power present at the received signal. The experiment undertaken have clearly shown the effect a ZigBee interferer has on BLE 4 and BLE 5 communication. Figure 31 and Figure 32 show the received signal power over the link distance. It can be clearly seen that RSSI value is stronger when the interferers are closer to scanner. This clearly indicates that RSSI estimation includes interferer signal power.

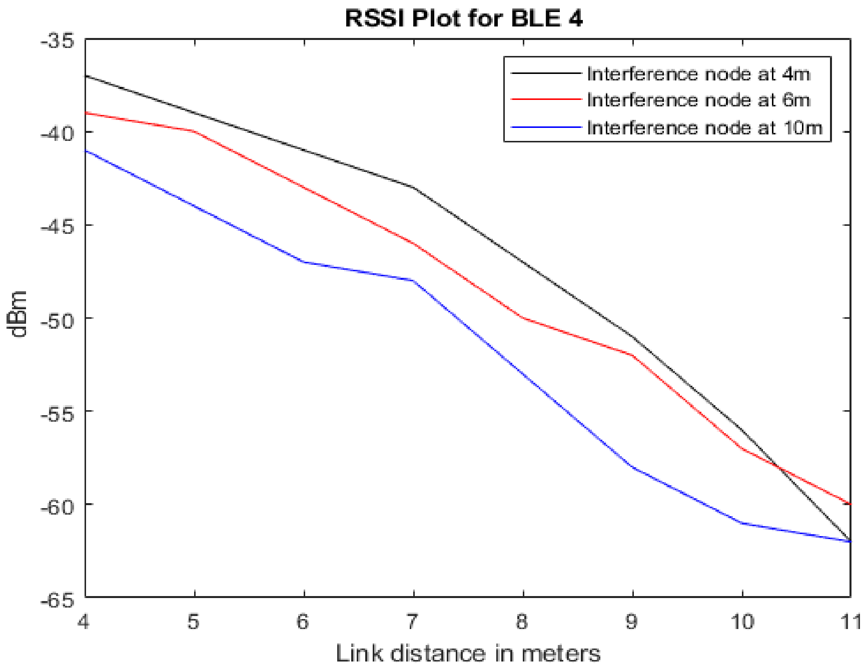

Figure 31. RSSI plot of BLE 4 over link distance.

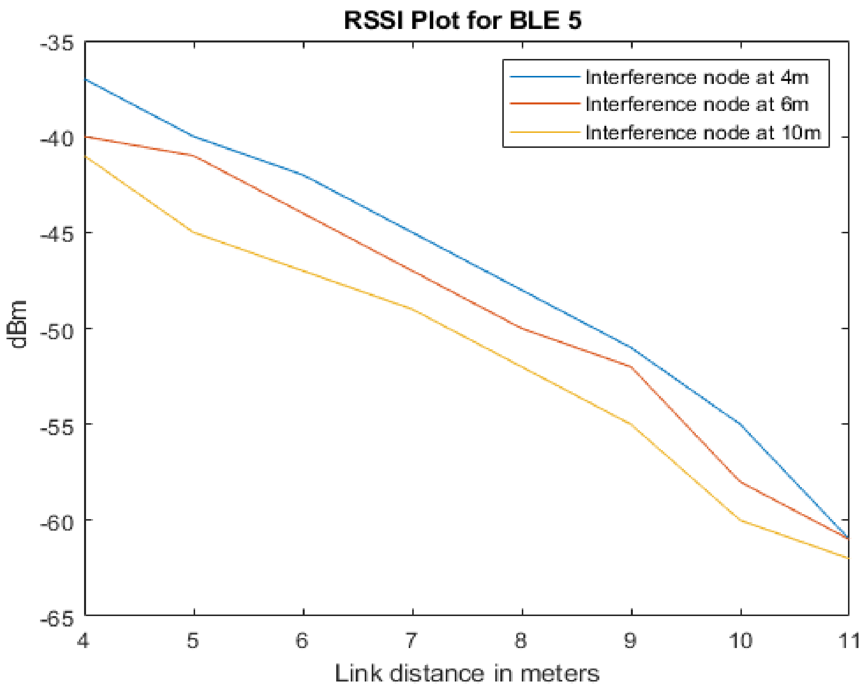

Figure 32. RSSI plot of BLE 5 over link distance.

Figure 31 and Figure 32 has the similar nature of RSSI plot for the both technologies with some minor changes. These difference in RSSI values could be due to the physical environment as well radio environment. Physical environment indicates the distance between advertiser and scanner. During experiment, position of antenna was changed as the interferers as well as device had to be moved while taking measurements. There is effect on data integrity of BLE 4 and BLE 5 based localization system, since interference effect on the RSSI of correctly received packets. On the other side, as the ZigBee signal interference is strong, the loss in packet received is more. This could lead to worse latency in the presence of interference due to increased packet loss.

6. DISCUSSION AND FURTHER WORK

As this thesis work was experiment-based, many challenges were faced during measurements and many questions arises in mind initially. During measurement period, for every measurement scenario there was a slight variation in the number of received packets. As the various environmental dimensions like position of the device, position of interferer changes, the measurement result varies. Another question arises in mind was that can Bluetooth data rate get faster? BLE is enough to provide higher data rates as comparison to classical Bluetooth, but as the time pass, there will be requirement for the more sensitive and complex application, for example medical devices. Although frequency-hopping spread spectrum practices greatly in resisting interference, it only uses one frequency channel at a time for transmission of data which results in lowered data rates. Modifications of the technology require changes in hardware as well as software but for the sustainability of the BLE it is necessary to find a way to achieve coexistence between technologies as the numerous applications will be required soon.

BLE 5 represents another step change in Bluetooth technology. The long-range Coded PHY is covering home and building automation with sensors of various types. Also, lightening, heating and air-conditioning all controlled by Bluetooth. Further, outdoor applications on transportation, gardens, restaurants, watch towers, Park, lake and many more field is possible with long-range covering. The higher symbol rate of LE 2M improves spectral efficiency and supports emerging use applications in sports, fitness, and complex medical equipment. For the next generations, Bluetooth extension in advertisements will pave the wave with advanced applications in audio system, personal gadgets, industries, and some smart city applications too. Further, BLE 5 is not only a promising technology to maintain superiority in commercial applications, it also targets the expansion possibilities for developing environmentally friendly sustainable applications. Although- future is hard to predict- BLE 5 has made itself a strong competitor for providing complete solution for IoT and, will have a sustainable impact in many sectors and future position it as the low power wireless technology of choice for the IoTs.

Further, how secure is Bluetooth, to fulfil the requirements of IoT? As referred to SIG, Bluetooth is targeting the market of industrial IoT. As mentioned, the secure and reliable communication matters most for the industrial applications. The optimized mesh technology is promising for resisting attacks, but many kinds of threats is there for the Bluetooth-based networks, such as jamming attack in device-intensive applications. Privacy regarding flooding-based networks is another issue, as there is possibility of all message receiving by any node in the coverage range.

BLE 5 appears to offer significance performance improvements as compared to the previous versions of Bluetooth. Considering significance improvements in speed, power consumption, range, and broadcasting capacity, BLE 5 seems to be strong candidate and one of the best choices for the IoT. Some of the technical challenges for the future IoT could be efficiency in communication, interoperability, scalability, ubiquity, secure access, and data mining. So, as BLE 5 being strong candidate, now the above-mentioned challenges associated with IoT becomes a research topic for the researchers.

Another further work in Bluetooth technology can be regarding energy efficiency. Thousands of sensors will be working simultaneously for the implementation of IoT, so energy efficient technology will be preferred. BLE usage of duty-cycled mode to cut down the operating time of device results in power saving and Bluetooth mesh heterogeneous network structure is advantageous for making energy efficient system.

An experimental result from a set up that consider LOS propagation has been shown in this thesis paper to evaluate the performance of BLE 5 technique under ZigBee interference. This experiment exhibits only a moderate range communication between the devices. One further work could be with NLOS propagation. For example, multi-floor scenarios with ZigBee as well as Wi-Fi scenario.

The implementation of IoT application will be massive and in numerous areas. Several short-range and long-range coverage technologies will be required for the implementation. Technologies like ZigBee, Wi-Fi, and many more are competing for the short-range applications and on the other side LPWANs like LoRa, NB-IoT are fulfilling long-range communication.

7. SUMMARY

In the present time, number of technologies are utilizing unlicensed RF spectrum in 2.4 GHz band. Among them, number of applications has been developed utilizing Bluetooth technology in order to make human life more comfortable as well as eco-friendly. A series of Bluetooth updates has been made by SIG in past 25 years. Among different Bluetooth versions, BLE series features low power consumption, low cost, faster connectivity, secure connection, as well as interoperable. BLE 5 aims to provide 4 times range, 2 times speed and 8 times broadcasting message capacity with increased functionality to provide reliable IoT connections. BLE 5 defines LE 1M, LE 2M and LE 3M coded (S = 8) PHY options with data rates of 1Mbps, 2Mbps, and 125 Kbps respectively. BLE technology is utilized into many products from mobile phones to complex medical devices so as to share the data among paired devices. As the number of technologies are utilizing 2.4 GHz ISM band, achieving coexistence between them is necessary. So these technologies must co-operate with each other in order to minimize the generated interference due to simultaneous application running in devices utilizing ISM band.

The main objective of this thesis was to evaluate the performance of BLE 5 technique under interference. A suitable measurement set-up was proposed, which includes two nRF52840 chipset developed by Nordic Semiconductors, three ZigBee sources to introduce interference, a sniffer to find out interference other than ZigBee, one laptop with installed HTerm terminal program, batteries as power source, and wireless USB cables for connection. Three different test measurements were performed with different ZigBee interference distances at 4 m, 6 m, and 10 m. The link distance was between 4 to 14 meters. The measurement was LOS and in open space. ZigBee was the only interferer at the time of measurement.

Performance measurement of BLE 4 and BLE 5 were performed. Different PHY specification has been defined to the different versions of Bluetooth. In comparison to the Bluetooth 4, Bluetooth 5 adds two new PHY variant. The PHY can be named as LE 1M (mode1), LE 2M (mode2), and LE coded (mode3). GFSK modulation scheme is used and operates as LE 1M, LE 2M and LE coded (S = 8) with a data rates of 1 Mbps, 2 Mbps and 125 Kbps respectively.

Results show that the worst-case interference is very harmful for BLE communication even when using the BLE 5 coded mode. Here, the worst-case interference refers when the interferers are at the same channel resulting in collision of useful signal and full packet. In terms of BLE link distance, the error correction coding gain was found to be 30 to 40 % (approximately one third of the used communication ranges). Results highlight that it is very important to pay attention to different technologies coexistence since, the amount of IoT devices is increasing rapidly creating interference to each other.

Resilience towards interference is especially important in applications which require highly reliable communication. Erroneous packet receptions will also decrease the energy efficiency which is highly important in IoT applications. Result of this thesis show that the BLE communication performance will decrease drastically if there are interfering ZigBee nodes in a close vicinity (< 6 m) at the same frequency channel. In future studies were going to evaluate different coexistence scenarios using analytical modelling and experimental measurements.

8. REFERENCES

[1] Heydon, R.(2013). Bluetooth Low Energy: The Developer's Handbook. New Jersey, USA: Prentice Hall Publishing.

[2] Gupta, N.C.(2013). Inside Bluetooth Low Energy. Boston, London: Artech House publishing.

[3] Davidson, R., Cufi, C., Akiba, & Townsend, K.(2014). Getting Started with Bluetooth Low Energy. Sebastopol, USA : O'Reilly Media, Inc Publishing.

[4] Suraj, C., Tejas, R., Shubham, S., Mayur, M., & Satish, Y. (2017). Survey Paper on Internet of Things. *KJs College of Engineering and Research IJESC*, 7(4), 10564-10567.

[5] Yin, J., Yang, Z., Cao, H., Liu, T., Zhou, Z.& Wu, C. (2019). A Survey on Bluetooth 5.0 and Mesh: New Milestones of IoT, *ACM Transactions on Sensor Networks*, 15(3), 1-29.

[6] Karvonen, H., Mikhaylov, K., Acharya, D., & Rahman, M. (2018). Performance Evaluation of Bluetooth Low Energy Technology under Interference, *13th EAI International Conference on Body Area Networks,* Oulu, Finland, 1-10. doi:10.1007/s11277-016-3335-4

[7] Karvonen, H., Mikhaylov, K., Hamalainen, M., Iinatti, J. & Pomalaza-raez, C. (2017). Experimental Performance Evaluation of BLE 4 vs BLE 5 in Indoors and Outdoors Scenarios, *International Conference on Body Area Networks,* Dalian, China. 1-7. doi: 10.475/123_4

[8] Nordic Semiconductors. (2019). nRF52840 Product Specification. Retrieved February 26, 2019, Available at: http://www.nordicsemi.com/eng/Products/nRF52840

[9] Woolley, M. (2019). Bluetooth 5 Go Faster. Go Further, Bluetooth SIG. Retrieved August 15, 2019, Available at: http://www.bluetooth.com/bluetooth-resources/bluetooth-5-go-faster-go-further/

[10] Bluetooth SIG. (2019). Bluetooth Core Specifications v 5.1. Retrieved February 28, 2019, Available at: http://www.bluetooth.com/specifications/Bluetooth-core-specification/

[11] Woolley, M. (2019). Bluetooth Core Specification 5.0 Feature Overview. Retrieved May 10, 2019, from http://www.bluetooth.com/bluetooth-resources/bluetooth--core-specification-v5-1-feature-overview/

[12] Woolley, M. (2017). Exploring Bluetooth 5- Going the distance. Retrieved March 5, 2019, Available at: https://www.bluetooth.com//blog/exploring-bluetooth-5-going-the-distance/

[13] IEEE Computer Society. (2003). IEEE standard 802.15.4 ™. 3 Park Avenue, New York, USA: The Institute of Electrical and Electronics Engineers, Inc.

[14] MathWorks, (2019). BLE channel selection algorithms. Retrieved June 1, 2019, Available at: https://www.mathworks.com/help/comm/examples/ble-channel-selection-algorithms.html

[15] Bluetooth SIG, (2019). Bluetooth. Retrieved June 10, 2019, Available at: https://www.bluetooth.com/

[16] Silicon labs, (2019). Bluetooth Low Energy. Retrieved June 25, 2019, Available at: https://www.silabs.com

[17] Baert, M., Rossey, J., Shahid, A., & Hoebeke, J. (2018). The Bluetooth Mesh Standard: An overview and experimental evaluation. *Sensors 2018*, 18(8), 1-24.

[18] Silva, S., Soares, S., Fernandes, T., Valenta, A., & Moreira, A. (2014). Coexistence and interference tests on a bluetooth low energy front-end, *Science and Information Conference (SAI)*, London, UK. 1014-1018. doi: 10.1109/SAI.2014.6918312

[19] Karvonen, H., Hämäläinen, M., Iinatti, J., & Pomalaza-Raez, C. (2017). Coexistence of Wireless Technologies in Medical Scenarios, *European Conference on Networks and Communicaiton Technology (EUCNC)*, Oulu, Finland. doi:10.1109/EuCNC.2017.7980774

[20] Yang, D., Xu, T., & Gidlund, M. (2011).Wireless coexistence between IEEE Std. 802.11- and IEEE Std. 802.15- based networks: A survey. *International journal of Distributed sensor networks*, 7(1), 1550-1329.

[21] Natarajan, R., Zand, P., & Nabi, M. (2016). Analysis of coexistence between IEEE Std. 802.15.4, BLE and IEEE Std. 802.11 in the 2.4 GHz ISM band. *42th conference of IEEE Industrial Electronics* Society (IECON 2016), Florence, Italy. 6025-6032. doi:10.1109/IECON.2016.7793984

[22] Hayajneh, T., Almashaqbeh, G., Ullah, S., & Vasolalps, A. (2014). A survey of wireless technologies coexistence in WBAN: analysis and open research issues. *Wireless Networks,* 20(8), 2165-2199.

[23] Karvonen, H., Hämäläinen, M., Iinatti, J., & Pomalaza-Raez, C. (2017). Interference of Wireless Technologies on BLE Based WBANs in Hospital Scenarios. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC),* Montreal, QC, Canada. 8-13 Oct. doi: 10.1109/PIMRC.2017.8292333

[24] Conti, A., Dardari, D., Pasolini, G., & Andrisano, O. (2003). Bluetooth and IEEE Std. 802.11b coexistence: analytical performance evaluation in fading channels. *IEEE Journals on Selected Areas in Communicaiton*, 21(2), 259-269.

[25] Sanctis, M. D., Monti, M., Ruggieri, M., & Prasad, R. (2009). A collaborative coexistence mechanism for IEEE Std. 802.15.3 and IEEE Std. 802.15.4 WPANs. *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, Tokyo, Japan. 395-399. doi: 10.1109/PIMRC.2009.5449885

[26] Sklar, B. (2001). *Digital Communication: Fundamentals and Applications*. California, USA: Prentice Hall Publishing.

[27] Kleer. (2007). ISM Band Coexistence Whitepaper. Retrieved August 10, 2019, Available at: ww1.microchip.com/downloads/en/DeviceDoc/Kleer_ISM_Coexistence.pdf

[28] Zacharies, S., Newe, T., O'keeffe, S., & Lewis, E. (2012). Coexistence measurements and analysis of IEEE Std. 802.15.4 with Wi-Fi and bluetooth for vehicle networks. *12th International Conference on ITS Telecommunications*, Teipei, Taiwan. 785-790. doi: 10.1109/ITST.2012.6425289

[29] Carhacioglu, O., Zand, P., & Nabi, M. (2017). Time-domain cooperative coexistence of BLE and IEEE Std. 802.15.4 networks. *IEEE 28th Annual International Symponium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Montreal, QC Canada. doi:10.1109/PIMRC.2017.8292262

[30] Garroppo, R., Gazzarrini, L., Giordano, S., & Tavanti, L. (2011). Experimental assessment of the coexistence of Wi-Fi, ZigBee, and Bluetooth devices. *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Lucca, Italy. doi: 10.1109/WoWMoM.2011.5986182

[31] Virk, M. H., Vuohtoniemi, R., Hämäläinen, M., Mäkelä, J.P., & Iinatti, J. (2014). Spectrum Occupancy Evaluations at 2.35-2.50 GHz ISM Band in a Hospital Environment. *Proceedings of the 9th International Conference on Body Area Networks*, London, United Kingdom. 39-45. doi: 10.4108/icts.bodynets.2014.256965

[32] Fotouhi, H., Causevic, A., Vahabi, M., & Bjorkman, M. (2016). Interoperability in heterogeneous Low-Power Wireless Networks for Health Monitoring Systems. *IEEE International Conference on Communications Workshops(ICC),* Kuala Lumpur, Malaysia. doi: 10.1109/ICCW.2016.7503819

[33] Nordic Semiconductors. (2018). nRF52840 Preview DK. Retrieved April 10, 2019, Available at: http://infocenter.nordicsemi.com/pdf/nRF52840_PDK_User_Guide_v1.2.pdf.

[34] Mikhaylov, K. (2018). *Plug And Play Reconfigurable Solutions For Heterogeneous IoT*. Oulu, Finland: University of Oulu Publishing.

[35] Mikhaylov, K., & Petäjäjärvi, J. (2017). Design and Implementation of The Plug&Play Enabled Flexible Modular Wireless Sensor and Actuator Network Platform: Design and Implementation of Plug&Play enabled Modular WSAN Platform. *Asian Journal of Control,* 9(14), 1392-1412.

[36] Texas Instruments. (2019). CC2650. Retrieved August 20, 2019, Available at: http://www.ti.com/product/CC2650#

[37] ZigBee Alliance. (2019). ZigBee. Retrieved July 10, 2019, Available at: http://www.zigbee.org/.

[38] Mouser Electronics. (2019). Taoglas, FXP70 data sheet. Retrieved Sep 1, 2019, Available at: https://www.mouser.fi/datasheet/2/398/FXP70.07.0053A-1508307.pdf.

[39] HTerm. (2019). HTerm. Retrieved Sep 10, 2019, Available at: http://www.der-hammer.info/terminal/

9. APPENDICES

Operation of the scanner is presented as a high-level algorithm which can be listed as follows,

```
Initialization procedures
while (button pressed)
        blink 4 LEDs
end(while)
operation mode = ID of the pressed button
send “Initialized” message over the serial interface
last_packet_ID =0;
packets_received =0;
start scanner
while(1)
    if (advertisement received)
        decode  data of an advertisement packet
        if(header==correct)
                last_packet_ID==ID of the current packet;
                packets_received++;
                last_packet_RSSI== RSSI of the current packet;
         end(if)
     end (if)
     if (one second from previous report has passed)
        report last_packet_ID over serial interface
        report packets_received over serial interface
        report last_packet_RSSI over serial interface
      end(if)
end(while)
```

Operation of the advertiser is presented as a high-level algorithm which can be listed as follows,

```
Initialization procedures
while (button pressed)
         blink 4 LEDs
end (while)
operation mode== ID of the pressed button
send “initialized” message over serial interface
counter==1
while (1)
        encode header and counter into manuf. Data of an advertisement packet
        send advertisement packet
        blink a LED (operation_mode)
```

```
        counter++
        wait (50ms)
        if (one second from previous report has passed)
                report number of sent advertisements over serial interface
        end (if)
end (while)
```